VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

AKVIZICE SLUŽBY PRO ZABEZPEČENÍ EMAILOVÉ KOMUNIKACE DLE ISMS

ACQUISITION OF EMAIL COMMUNICATION SECURITY SERVICE ACCORDING TO ISMS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Adam Foltýn**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Adam Foltýn**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2017/18

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Akvizice služby pro zabezpečení emailové komunikace dle ISMS

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

V diplomové práci se budu zabývat návrhem akvizice vhodného řešení pro zabezpečení emailové komunikace, která je jedním z klíčových komunikačních kanálů ve sledované společnosti, dle ISMS.
V teoretické části bude shrnuta potřebná teorie včetně vysvětlení nezbytných základních pojmů, důležitých pro pochopení následujících částí práce. Bude se jednat převážně o témata spojená s ISMS, emailovou komunikací a principy řízení informační bezpečnosti dle norem řady ISO/IEC 27 000.
V části analýza současného stavu popíši současnou situaci ve sledované společnosti, její předmět podnikání, organizační strukturu, hlavní procesy odehrávající se uvnitř společnosti. Bude zde také popsáno hardwarové a softwarové vybavení společně s bezpečnostními politikami, řízením lidských zdrojů včetně přístupů a fyzické zabezpečení společnosti – vše s ohledem na informační bezpečnost.
V části práce zabývající se návrhem vlastního řešení poté provedu analýzu rizik opírající se

o informace uvedené v části analýza současného stavu. Na základě zjištěných výsledků bude poté proveden výběr vhodných bezpečnostních opatření z oblasti zabezpečení emailové komunikace v podobě služeb zabezpečujících emailovou komunikaci, jejich srovnání a výběr jedné, která bude společnosti doporučena k akvizici.
Výstupem diplomové práce bude doporučení pro sledovanou společnost v oblasti akvizice služeb sloužících k zabezpečení emailové komunikace, kdy dle výsledků získaných v části návrhu vlastního řešení bude společnosti doporučena jedna ze služeb včetně zdůvodnění jejího výběru a ekonomického zhodnocení.

Základní literární prameny:

ČSN ISO/IEC 27001: Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, Petr. Řízení bezpečnosti informací. 2. přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80- 7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2017/18.

V Brně, dne 28. 2. 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA PODNIKATELSKÁ

L.S.

B. Půža

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

Abstrakt

Diplomová práce se zabývá návrhem akvizice služby pro zabezpečení emailové komunikace dle ISMS ve společnosti, zprostředkovávající obchodování na finančních trzích. Práce je rozdělena do tří částí. V teoretické části jsou uvedeny pojmy a vysvětlena teoretická východiska, jejichž znalost je nutná k realizaci dalších částí práce. V analytické části je popsán současný stav společnosti vzhledem k informační bezpečnosti. V rámci části návrhu vlastního řešení je provedena analýza rizik, na jejímž základě jsou poté navrhnuty vhodné varianty zabezpečení emailové komunikace včetně ekonomického zhodnocení.

Abstract

The diploma thesis focuses on a proposal of acquisition of email communication security service according to ISMS for a company which provides trading services on financial markets. The thesis is divided into three parts. In the theoretical part, necessary terms and theoretical essentials are explained in order to ensure understanding of the following parts of the thesis. The following analytical part describes the company's current security status of information. As a solution in the final part of the thesis, partial risk analyses are conducted. Based on these, suitable options for email communication security measures are proposed as well as their the economical evaluation.

Klíčová slova

ISMS, informační bezpečnost, bezpečnost podniku, analýza rizik, bezpečnostní opatření, ISO/IEC 27 000

Keywords

ISMS, information security, company security, risk analyses, security measures, ISO/IEC 27 000

Bibliografická citace práce

FOLTÝN, A. Akvizice služby pro zabezpečení emailové komunikace dle ISMS. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 81 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 3.5.2018

……

Bc. Adam Foltýn

Poděkování

Rád bych tímto poděkoval všem, kteří mě při tvorbě této diplomové práce podporovali a to především svému vedoucímu diplomové práce panu Ing. Petru Sedlákovi za odborné vedení, rady a vstřícnost. Dále pak zkoumané společnosti za to, že mi umožnila realizaci diplomové práce v rámci svého působení a za veškeré poskytnuté informace, které byly při tvorbě této práce použity. Děkuji také mým rodičům, kteří mě během celé doby studia na vysoké škole podporovali.

OBSAH

ÚVOD

Dnešní dobu lze zcela jistě nazvat dobou informační, jelikož informace jsou dostupné všude kolem nás a staly se také nedílnou součástí každé organizace, kdy ve většině případů představují to zcela nejcennější aktivum, kterým daná organizace disponuje. Stejně tak jako se rozvíjí využití, zpracování a analýzy nashromážděných dat ze strany organizací, rozvíjí se i tendence útočníků na tyto informace útočit, krást je a zneužívat ke svému vlastnímu obohacení nebo k dosažení konkurenční výhody. Dnes se proto řízení informační bezpečnosti stává více než kdy jindy nutnou součástí celofiremních strategií a i sami organizace si začínají uvědomovat důležitost ochrany a správného nakládání s vlastními daty. Drtivá většina společností také využívá při svém fungování více informačních a komunikačních kanálů, které je třeba chránit, jelikož i malý únik citlivých informací zde může představovat vážnou hrozbu jak z hlediska reputace společnosti, tak i z případných legislativních a právních následků, které pro společnost mohou v důsledku ztráty informací vyplynout.

Informační bezpečnost lze poměrně snadno realizovat na technické úrovni, jelikož zde existují softwarová i hardwarová řešení a tak se zde více než kde jinde uplatňuje hlavní poučka informační bezpečnosti, kterou je, že bezpečnost je silná pouze tak, jako její nejslabší článek, který zde představuje člověk.

Tato diplomová práce je rozdělena do tří částí, přičemž první část se zaobírá teoretickými východisky, nutnými k pochopení dalších částí práce, kterými jsou analýza současného stavu ve zkoumané společnosti a návrh vlastního řešení, jehož výstupem je doporučení pro zvýšení bezpečnosti v oblasti emailové komunikace mezi klienty a zkoumanou společností.

CÍLE PRÁCE

V diplomové práci se budu zabývat návrhem akvizice vhodného řešení pro zabezpečení emailové komunikace, která je jedním z klíčových komunikačních kanálů ve sledované společnosti, dle ISMS.

V teoretické části bude shrnuta potřebná teorie včetně vysvětlení nezbytných základních pojmů, důležitých pro pochopení následujících částí práce. Bude se jednat převážně o témata spojená s ISMS, emailovou komunikací a principy řízení informační bezpečnosti dle norem řady ISO/IEC 27 000.

V části analýza současného stavu popíši současnou situaci ve sledované společnosti, její předmět podnikání, organizační strukturu, hlavní procesy odehrávající se uvnitř společnosti. Bude zde také popsáno hardwarové a softwarové vybavení společně s bezpečnostními politikami, řízením lidských zdrojů včetně přístupů a fyzické zabezpečení společnosti – vše s ohledem na informační bezpečnost.

V části práce zabývající se návrhem vlastního řešení poté provedu analýzu rizik opírající se o informace uvedené v části analýza současného stavu. Na základě zjištěných výsledků bude poté proveden výběr vhodných bezpečnostních opatření z oblasti zabezpečení emailové komunikace v podobě služeb zabezpečujících emailovou komunikaci, jejich srovnání a výběr jedné, která bude společnosti doporučena k akvizici.

Výstupem diplomové práce bude doporučení pro sledovanou společnost v oblasti akvizice služeb sloužících k zabezpečení emailové komunikace, kdy dle výsledků získaných v části návrhu vlastního řešení bude společnosti doporučena jedna ze služeb včetně zdůvodnění jejího výběru a ekonomického zhodnocení.

1 TEORETICKÁ VÝCHODISKA

V této části práce budou představena teoretická východiska a poznatky týkající se problematiky, jenž je řešena v následujících částech práce. Bude se konkrétně jednat o představení základních pojmů a názvosloví, nutného pro objasnění významu používaných pojmů. Dále poté teoretické podklady týkající se oblasti ISMS, problematiky nově v platnost vstupujícího evropského nařízení GDPR, norem řady ČSN ISO/IEC 27000, základní problematiky emailové komunikace a principy analýzy rizik z pohledu informační bezpečnosti.

1.1 Seznam pojmů a názvosloví

Vzhledem k množství využívaných odborných termínů v rámci práce a jejich možnému více významovému vyložení shrnuje následující část práce klíčové pojmy včetně jejich definic.

Akceptace rizik – rozhodnutí o přijetí/podstoupení daného rizika. [5]

Aktivum – cokoliv, co má pro společnost materiální nebo duševní hodnotu. Může se tedy jednat jak o hmotný, tak i nehmotný statek. [5]

Analýza rizik – systematický proces, během kterého jsou využívány získané informace pro odhad míry případného rizika a jeho zdrojů. [5]

Bezpečnost informací – proces, jehož výsledkem je ustanovení zásad pro nakládání s informacemi v podobě dat v digitálním i nedigitálním formátu a jejich správy. Bezpečnost informací v sobě obsahuje bezpečnost IS/ICT. Jedná se o podmnožinu bezpečnosti organizace. [4]

Bezpečnost IS/ICT – klade si za cíl ochranu aktiv, jenž jsou uložena v rámci informačního systému společnosti, který je podporován informačními a komunikačními technologiemi z prostředí společnosti, ale i jejího okolí. Jedná se o podmnožinu bezpečnosti informací a bezpečnosti organizace. [4]

Bezpečnost organizace – systém zabezpečení veškerého majetku a zajištění bezpečnosti organizace vzhledem k vnějšímu i vnitřnímu prostředí společnosti. Obsahuje bezpečnost informací a bezpečnost IS/ICT. [4]

Bezpečnostní incident – narušení bezpečnosti informací z pohledu dostupnosti, důvěrnosti nebo integrity. [1]

Bezpečnostní událost – událost, jejímž následkem může dojít ke vzniknu bezpečnostního incidentu. [1]

Cloud – dodávání výpočetních služeb různých typů skrze prostředí internetu. [7]

Data – informace uložené ve formě statických záznamů, odrážející určitý stav reality v daném časovém okamžiku jejich zaznamenání. [6]

Dostupnost – schopnost zajistit dostupnost k určité informaci v požadovaném čase pro oprávněného uživatele. [5]

Důvěrnost – schopnost zajištění přístupu k informaci pouze oprávněnému uživateli. [5]

GDPR – obecné nařízení na ochranu osobních údajů (ang. General Data Protection Regulation), jedná se o právní rámec ochrany osobních údajů v evropském prostoru s cílem hájit práva občanů EU proti neoprávněnému zacházení s jejich daty včetně osobních údajů. [8]

Hodnocení rizik – proces analýzy a vyhodnocení rizik vzhledem k jejich potenciálnímu dopadu a pravděpodobnosti výskytu. [5]

Hrozba – potenciální údalost, která může svým vznikem ohrozit bezpečnost. [5]

Informace – význam přisouzený datům, který je vhodný pro pozdější rozhodovací proces, kdy je na základě schopností osoby v rozhodovací roli takto extrahovaný význam z dat využit. Pro někoho se tedy můžou určitá data jevit jako bezvýznamná, jelikož daný člověk z nich není schopen získat význam nebo nerozumí významu uloženému v těchto datech. [6]

Informační management – činnosti, jejichž cílem je určité požadované zpracování dat v organizaci nebo vytváření těchto dat. Jsou přitom zahrnuty veškeré úlohy managementu, které se týkají získávání, zpracování, přenosu a uložení informací. [6]

Informační systém – soubor lidských a technických zdrojů společnosti a metod pro sběr, přenos, uchování a zpracování dat za účelem prezentace výstupů z takto zpracovaných dat jednotlivým uživatelům informačního systému. [6]

Integrita – schopnost zajištění správnosti, celistvosti a úplnosti uložené informace. [5]

ISMS – systém řízení bezpečnosti informací (angl. Information Security Management System), který řídí bezpečnost informací z pohledu jejich dostupnosti, důvěrnosti a integrity. Je součástí celkového systému řízení organizace. [5]

Norma – doporučení pro daný standard nebo řešení nejčastěji ve formě směrnice, která doporučuje použitelné standardy pro realizaci požadovaného kompatibilního řešení. [5]

Opatření – vyvíjená aktivita, jejímž cílem je snížení hrozby. [5]

Riziko – vzniká kombinací hrozby a zranitelnosti s dopadem na příslušné aktivum. [5]

Řízení rizik – činnosti vedoucí k potřebnému řízení a kontrole organizace s ohledem na možný výskyt rizik. [5]

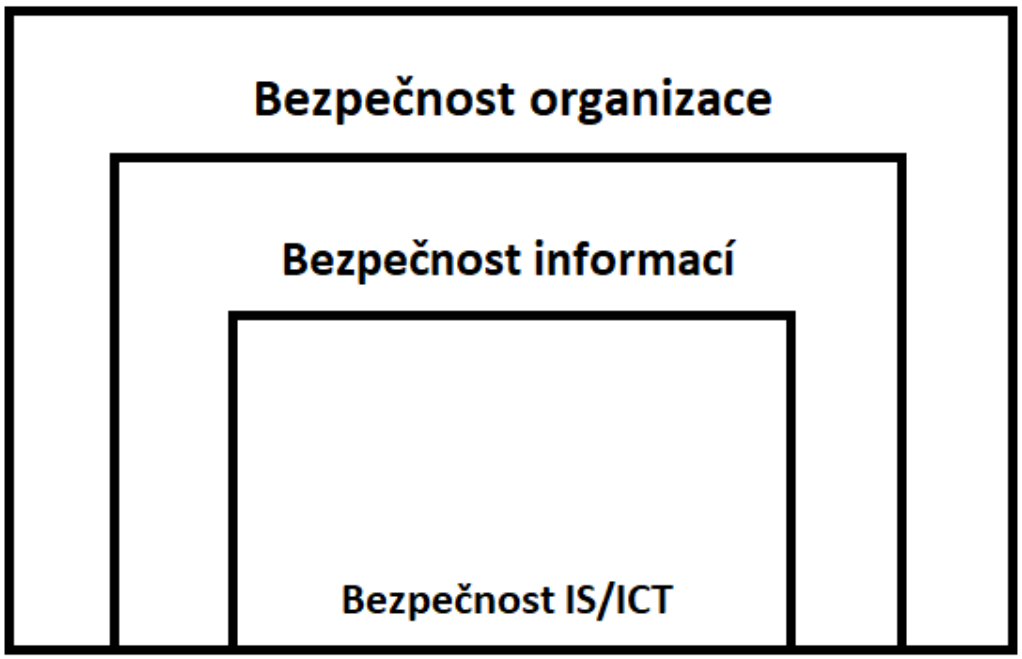
S/Mime – zkratka pro protokol Secure Multipurpose Internet Mail Extension. Protokol poskytující dodatečnou ochranu emailové komunikace na základě end-to-end šifrování. [9]

Standard – dokumentovaná úmluva obsahující jasně definované kritéria různého typu, která jsou využívána jako pravidla v rámci odvětví za účelem dosažení požadovaného výsledného stavu výrobků, služeb nebo procesů. [5]

Vyhodnocení rizik – proces, kdy je porovnáváno odhadnuté riziko s určenými kritérii za účelem jeho ohodnocení. [5]

Zranitelnost – slabé místo aktiva, na kterém lze očekávat působení hrozby. [5]

Zvládání rizik – proces výběru a přijímání opatření pro snížení rizika. [5]



Obrázek 1: Schéma bezpečnosti v organizaci (Zdroj: Vlastní dle 5)

1.2 Systém řízení bezpečnosti informací (ISMS)

V této části práce bude představen systém řízení bezpečnosti informací.

1.2.1 Definice ISMS

Systém řízení bezpečnosti informací (angl. Information Security Management System) je systémem řízení bezpečnosti informací v rámci organizace, který je nezbytně nutné chápat v souvislostech s celkovým řízením společnosti, jelikož jej nelze provozovat jako samostatnou součást bez provázání na další dílčí řídící procesy, probíhající v celé organizaci. ISMS se skládá z politik, postupů a směrnic, které na základě „best practises" doporučují činnosti vedoucí k jeho ustanovení, zavedení, řízení a kontrole tak, aby došlo ke splnění a kompatibilitě s mezinárodně uznávanými normami. Systém řízení bezpečnosti informací je tedy uceleným systematickým přístupem k ustanovení, implementaci, provozu, monitoringu, přezkoumání a zkvalitnění bezpečnosti informací v rámci společnosti. [1]

Norma řady ČSN ISO/IEC 27001:2014 poté definuje systém řízení bezpečnosti informací následujícím způsobem jako:

„Část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací.“ [2]

ISMS je založeno na posouzení rizik a na úrovních přijetí rizik organizace, které byly navrženy pro efektivní ošetření rizik a pro jejich řízení. [1]

Na ISMS lze také nahlížet jako efektivní dokumentovaný systém řízení a správy informačních aktiv společnosti s cílem eliminovat jejich možnou případnou ztrátu nebo poškození tím, že:

- určíme aktiva, která je potřeba chránit,
- zvolíme a řídíme možná rizika bezpečnosti informací,
- na zvolená rizika jsou navrhnuta adekvátní bezpečnostní opatření s dostatečnou úrovní záruk, která jsou kontrolována.

Systém řízení bezpečnosti informací pak může být zaveden plošně v rámci celé organizace, jen pro určitou složku organizace nebo informační systém organizace. V každém z těchto případu však rozhoduje o jeho zavedení a konečné odsouhlasení budování ISMS spadá do kompetence vrchního vedení společnosti, jelikož svojí povahou zasuhují tato rozhodnutí do strategického řízení společnosti. [5]

1.2.2 Etapy zavádění ISMS

Cílem zavádění ISMS by mělo být efektivní a systematické prosazení vybraných bezpečnostních opatření. [5]

Celý proces zavádění systému řízení bezpečnosti informací do provozu lze rozdělit do čtyř etap, kdy každá z nich obsahuje specifické činnosti, které je nutné vykonat ideálně na základě doporučení, jenž obsahují relevantní normy tak, aby bylo dosaženo požadovaného cíle v rámci každé z prováděných etap a ve výsledku tak celkově došlo k zavedení ISMS do běžného provozu společnosti. Doporučení pro ustanovení a implementaci ISMS dle souladu s požadavky normy ČSN ISO/IEC 27001:2014 poté obsahuje norma ČSN ISO/IEC 27003:2018. [3]

První etapa pro zavedení systému řízení bezpečnosti informací v rámci společnosti nebo jejího celku je zcela klíčová a týká se ustanovení o zavádění ISMS v rámci konkrétního

podniku, jenž musí být schváleno ze strany vedení společnosti. Schválení o zavedení ISMS ze strany vedení společnosti je požadováno normou a jedná se o první dokument, který bude požadován auditorem při auditu ISMS. Zavádění ISMS by mělo být realizováno směrem od vrchu dolů, čili od nejvyšších míst vedení až po nejnižší útvary působící v rámci společnosti. [5]

Druhou etapou v rámci zavádění ISMS je provedení identifikace aktiv včetně jejich ohodnocení a provedení celkové analýzy rizik za účelem zjištění potenciálních hrozeb a zranitelností identifikovaných aktiv. Identifikace aktiv by měl být systematický proces založený na předem definovaném algoritmu pomocí kterého budou nejprve identifikována z hlediska bezpečnosti relevantní aktiva a poté těmto aktivům přiřazena hodnota vzhledem k základním parametrům informační bezpečnosti (důvěra, dostupnost, integrita). Analýza rizik je poté druhým procesem, který následuje za identifikací aktiv, v rámci kterého jsou určeny potenciální rizika a dopady s nima spjatá. Analýza rizik je klíčový dokument v rámci zavádění ISMS a na jeho korektním vypracování by si měla dát společnost potažmo implementační tým záležet, jelikož jeho nesprávné zpracování může přinést značné problémy. [5]

Třetí etapou je provedení návrhu opatření, kdy jsou na základě provedené identifikace aktiv a vypracováné analýzy rizik navrhnuta bezpečnostní opatření na zjištěná rizika a případná kritická místa tak, aby umožňovala zjištěná rizika efektivně eliminovat. Společnost se za určitých okolností může rozhodnout zjištěná rizika akceptovat, tj. podstoupit je. S touto etapou je také spojena tvorba dokumentu Prohlášení o aplikovatelnosti, v němž jsou zdokumentovány cíle jednotlivých bezpečnostních opatření a jakým způsobem jsou které části ISMS zavedeny. [5]

Čtvrtou etapou v rámci zavádění ISMS, která je ovšem oproti třem předchozím nepovinná je certifikace zavedeného ISMS. ISMS může fungovat i bez certifikace. Certifikace probíhá ve dvou částech, kdy je během první části zcertifikována dokumentace a ve druhé části poté praktické zavedení ISMS v provozu. [5]

1.2.3 Povinná ISMS dokumentace

Zavádění ISMS musí být náležitě zdokumentováno pro potřeby auditu, kdy musí dokumentace obsahovat veškerá rozhodnutí vedení společnosti společně s činnostmi pro zajištění jejich možné opakovatelnosti a zpětné dohledatelnosti. [4] Výčet povinných dokumentů je poté následovný:

- Rozsah a hranice ISMS
- Politika ISMS
- Definice přistupu k hodnocení rizik
- Identifikace a ohodnocení aktiv
- Identifikace rizik
- Analýza rizik
- Návrh opatření
- Cíle opatření a bezpečnostní opatření pro zvládání rizik
- Akceptace rizik
- Získání povolení k provozování ISMS v rámci organizace
- Prohlášení o aplikovatelnosti

1.3 PDCA cyklus

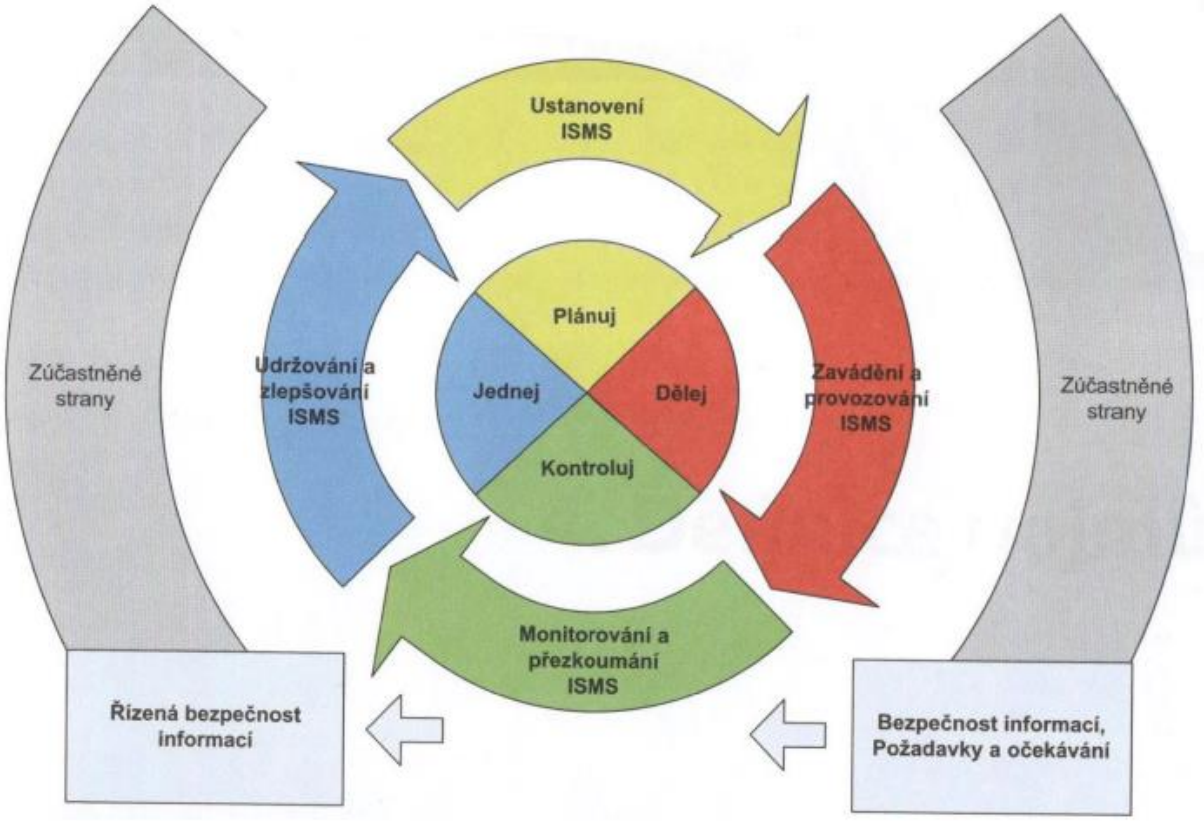
PDCA cyklus neboli také Demingův cyklus je manažerskou metodou využívanou v rámci managementu napříč různými obory a vyvinutou Williamem Edwardsem Demingem ve 20. století. [4]

Jedná se o metodu při které dochází ke kontinuálnímu zlepšování činností a procesů, které ovlivňují například kvalitu výrobků, služeb, aplikací nebo samotných procesů za pomocí čtyř neustále se opakujících činností [5]:

- Plan (plánování)
- Do (vykonávání)
- Check (kontroly)
- Act (jednání)

Pokud tak aplikujeme model PDCA na životní cyklus ISMS, dospějeme k závěru, že životní cyklus ISMS je na tomto modelu založen, jelikož sestává ze čtyř na sebe

navazujících, konjunktivních, nikdy nekončících etap, kterými jsou ustanovení ISMS, zavádění a provoz ISMS, monitorování a přezkoumání ISMS a udržování a zlepšování ISMS.



Obrázek 2: PDCA cyklus - životní cyklus ISMS (Zdroj: 5)

Ustanovení ISMS (plánování)

V rámci ustanovení ISMS se provádí vymezení hranic a rozsahu, kterého se bude ISMS týkat, společně s jasným manažerským zadáním, definicí a výběrem bezpečnostních opatření na základě identifikace a analýzy rizik. [6]

Zavádění a provoz ISMS (vykonávání)

V této etapě dochází k realizaci a prosazování bezpečnostních opatření na základě návrhu provedeného v rámci ustanovení ISMS. [4]

Monitorování a přezkoumání ISMS (kontrola)

Během této etapy dochází ke sbírání poznatků a zpětné vazby z již fungujícího a zavedeného ISMS. Poznatky takto zjištěné jsou poté vyhodnoceny a figurují v činnostech následující etapy.

Pro zajištění těchto poznatků je využíváno auditu, který zajišťuje systematický, dokumentovaný a nezávislý proces sběru informací včetně jejich objektivního vyhodnocení. [5]

Udržování a zlepšování ISMS (jednání)

Na základě poznatků získaných v předcházející etapě je poté realizováno možné zlepšení za účelem zvýšení bezpečnosti informací ve společnosti nebo odstranění zjištěných slabých míst a neshod s referenčními normami. [4]

Po ukončení poslední etapy se celý cyklus opakuje tak, aby bylo neustále dosahováno kvalitnějšího řízení ISMS v neustále se měnících a rychle se vyvíjejících podmínkách vnitřního i okolního prostředí společnosti.

1.4 Normy a normalizační instituce

V této části diplomové práce budou shrnuty teoretická východiska týkající se normalizačních institucí a jimi vydávaných norem, týkajících se oblasti informační bezpečnosti.

1.4.1 Normalizační instituce

V rámci normalizací standardů napříč ICT působí celosvětově několik významných normalizačních organizací, mezi které se řadí instituce ISO, IEC, ITU a rámci ČR poté ČSNI.

ISO – International Organization for Standardization

Jedna z největších a nejznámějších standardizačních organizací na světě, jejímž primárním cílem je podpora rozvoje standardizačních aktivit spojených se zaměřením na

usnadnění mezinárodní směny zboží, služeb a na spolupráci v intelektuální, vědecké a technologické sféře společně s ekonomickými aktivitami s nimi spojenými. [5]

IEC – International Electrotechnical Commission

Celosvětová standardizační organizace, která se zaměřuje na normalizační činnost především v rámci elektrotechnických a elektronických oblastí a oblastí jim podobných. [5]

ITU – International Telecommunications Union

Původně vzniklá organizace s účelem působení ve sféře telekomunikací, nicméně v dnešní době kdy běžně dochází k prolínání telekomunikací s informačními technologiemi se normy vydávané touto institucí uplatňují také v rámci prostředí ICT.

Organizace spadá svojí působností do hierarchie OSN, kde se již účastnila a podpořila rozšíření nových technologií, jakými jsou například mobilní či internetové technologie. Její současná činnost se věnuje základním stavebním prvkům současné globální informační infrastruktury a podílí se na tvorbě vyspělých multimediálních systémů s tím, že stále zastává roli přední organizace ve správě spekter radiových frekvencí. [5]

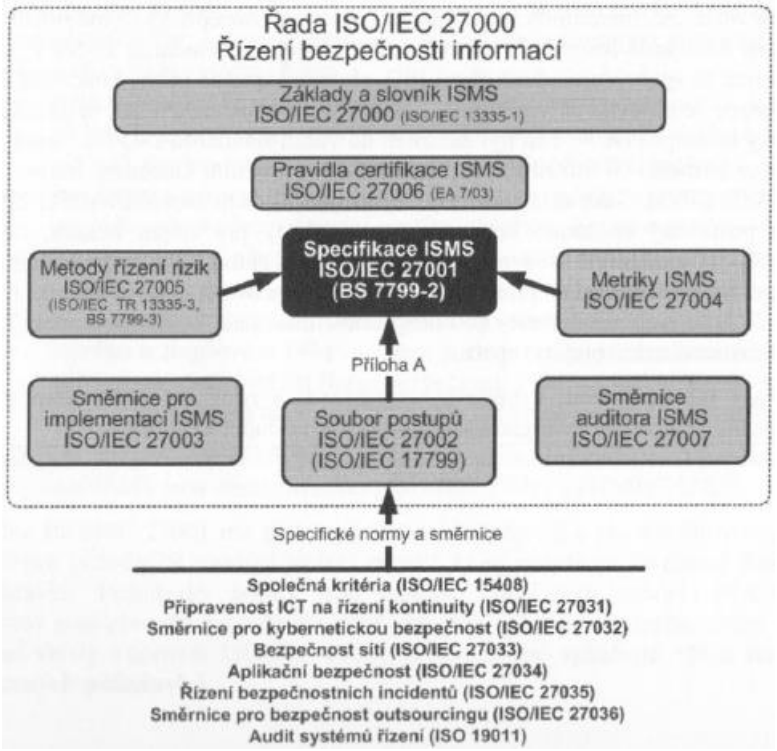
ČSNI – Český Normalizační Institut

Český normalizační institut vzniknul jako příspěvková státní organizace s cílem zastupovat a hájit národní zájmy u mezinárodních a evropských normalizačních institucí v pozici české národní normalizační instituce. V současné době organizace svým působením spadá pod správu Ministerstva průmyslu a obchodu a je zároveň členem mezinárodních a evropských normalizačních institucí ISO, IEC, CEN, CENELEC a ETSI. České normy, vydávané touto institucí poté vznikají jedním ze dvou způsobů a to buď přejímáním evropských a mezinárodních norem do soustavy českých technických norem formou ČSN EN (ČSN ISO, ČSN IEC, atd.) nebo tvorbou vlastních ČSN norem, jejichž vznik vyplývá z národních potřeb. [5]

1.4.2 Normy

V zásadě lze říci, že normy slouží k tomu, aby byly informační systémy a elektrotechnické výrobky od různých výrobců schopny mezi sebou komunikovat.

Většina mezinárodně uznávaných norem z oblasti informační bezpečnosti je založena na cyklu PDCA a jejich jádro tvoří normy řady ČSN ISO/IEC 27000. Normy této řady věnují velkou pozornost tomu, aby byly navrhnutá bezpečnostní opatření navázána na normy, které rozebírají určité oblasti bezpečnosti více do hloubky. Jádrem norem řady ČSN ISO/IEC 27000 je poté norma ČSN ISO/IEC 27001:2014, jenž definuje samotný systém řízení bezpečnosti informací ve společnosti. [4]



Obrázek 3: Normy řady ISO/IEC 27000 (Zdroj: 4)

ČSN ISO/IEC 27000:2017 Systémy řízení bezpečnosti informací – Přehled a slovník

Tato norma definuje a vysvětluje pojmy, které jsou poté využívány v celé rodině norem řady ČSN ISO/IEC 27000. Poskytuje také přehled systémů řízení bezpečnosti informací a společně s dalšími normami téže řady má pomoci společnostem všech typů a velikostí zavést a provozovat ISMS. [5]

ČSN ISO/IEC 27001:2014 Systémy řízení bezpečnosti informací – Požadavky

V rámci této normy jsou specifikovány požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a certifikaci ISMS ve zdokumentované podobě. Norma doporučuje zvolení procesního přístupu při řešení ISMS a zavádí přitom do praxe využití modelu PDCA. [5]

ČSN ISO/IEC 27002:2014 Systémy řízení bezpečnosti informací – Soubor postupů

Norma obsahuje směrnice pro organizační normy bezpečnosti informací a postupy jejich řízení. Směrnice společně s postupy jsou v rámci této normy definovány včetně výběru, implementace a řízení opatření. Zohledňuje přitom prostředí rizik bezpečnosti informací v dané organizaci. [19]

ČSN ISO/IEC 27003:2018 Směrnice pro implementaci systému řízení bezpečnosti informací

Norma se zabývá procesem zavedení ISMS do provozu už od jeho návrhu až po tvorbu implementačního plánu a zaměřuje se přitom na kritická místa, jenž mohou v rámci jednotlivých vykonávaných činností vzniknout. V rámci normy je definován proces získání souhlasu vedení společnosti o započetí projektu budování ISMS, definice rozsahu a hranic včetně analýzy požadavků na bezpečnost informací a s tím související analýzu rizik. Tato norma je aplikovatelná v prostředí jakékoliv organizace, přičemž samotné organizace si mohou normu poté adekvátním způsobem doplnit o své potřeby. [5]

ČSN ISO/IEC 27005:2013 Řízení bezpečnosti informací

Norma poskytuje doporučení pro řízení rizik vzhledem k informační bezpečnosti, přičemž podporuje v činnostech, spjatými s řízením rizik, uplatňování konceptu, zaneseného v normě ČSN ISO/IEC 27001:2014, tj. uplatňuje využívání PDCA modelu pro potřeby činností řízení rizik. K pochopení normy je nezbytná znalost norem ČSN ISO/IEC 27001:2014 a ČSN ISO/IEC 27002:2014 a to především konceptů, modelů a terminologie, které jsou v daných normách uvedeny. Tato norma nechává výběr přístupu k řízení rizik na dané organizaci a nenabízí tak jednu konkrétní metodiku. [5]

1.5 Aktiva

Identifikace a ohodnocení aktiv společnosti je nezbytnou a klíčovou součástí procesu zavádění ISMS a proto budou jeho teoretická východiska a postupy rozebrány v následující části práce.

1.5.1 Identifikace aktiv

Při identifikaci aktiv je nutné brát zřetel na skutečnost, aby byly do výčtu aktiv zahrnuta pouze aktiva, spadající do rozsahu zavádění ISMS a zároveň aktiva o dostatečném stupni podrobnosti a relevantnosti vzhledem k informační bezpečnosti a potřebám analýzy rizik. [15]

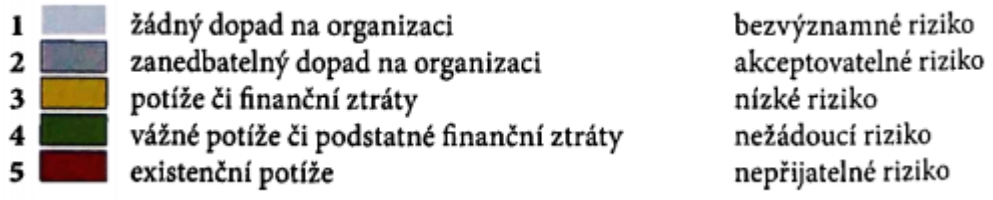
V rámci této etapy je pak hlavním úkolem logicky seskupit aktiva, která k sobě významově patří do skupin (například softwarové vybavení, hardwarové vybavení atd.). K takto seskupeným aktivům poté určit vlastníka, tj. zodpovědnou osobu, se kterou bude následně diskutována hodnota aktiva. [5]

Výstupem této činnosti je poté seznam aktiv, u kterých je zapotřebí zajistit řízení rizik včetně firemních procesů, jenž se k vybraným aktivům vztahují. [15]

1.5.2 Hodnocení aktiv

Při této etapě lze využít některý z dostupných profesionálních nástrojů určených k ohodnocení aktiva a pracujících na základě některé z metodik (hojně využívanou metodikou v této oblasti je CRAMM). [5]

Pro hodnocení aktiva je nutné vytvořit stupnici kvantitativního nebo kvalitativního charakteru, přičemž kvantitativní hodnocení bude oceňovat aktiva v domácí měně a kvalitativní na určité, předem definované stupnici. [5]



Obrázek 4: Příklad kvalitativní stupnice hodnocení aktiv (Zdroj: 5)

Hlavním principem hodnocení aktiv je vyčíslení nákladů, způsobených v důsledku narušení identifikovaných aktiv z pohledu jejich důvěrnosti, dostupnosti a integrity, přičemž ke každému z těchto prvků je v rámci jednoho aktiva přiřazena hodnota z vytvořené stupnice. [5]

Při výpočtu výsledné hodnoty aktiva lze využít více metod. Pro potřeby diplomové práce bude využita součtová metoda, která počítá hodnotu aktiva jako (důvěrnost + dostupnost + integrita) / 3. [5]

1.6 Analýza rizik

Analýza rizik slouží k identifikaci zranitelných míst identifikovaných aktiv společně s hrozbami, které na tyto místa působí. Jejím účelem je zdokumentování rizik v závislosti na hrozbách a pomocí vhodných opatření snížit dopady těchto rizik na minimum. [5]

K analýze rizik lze přistupovat čtyřmi přístupy:

- Analýza rizik – hrubá úroveň.
- Analýza rizik – neformální přístup.
- Analýza rizik – kombinovaný přístup.
- Analýza rizik – podrobný přístup. [5]

1.6.1 Analýza rizik – hrubá úroveň

Zaobírá se určením hodnoty IT systému společnosti z pohledu jejího fungování a zpracování informací. Určuje důležitost systému v rámci organizace z hlediska informační bezpečnosti. [5]

Jejím výstupem je tak seznam systémů, na které je vhodné aplikovat základní přístup analýzy rizik a na které bude zapotřebí využití podrobného přístupu, jelikož tento systém je z pohledu informační bezpečnosti kritický.

1.6.2 Analýza rizik – neformální přístup

Jedná se o analýzu provedenou na základě znalostí analytika, která je podpořena zároveň i znalostmi a zkušenostmi dalších zapojených osob. Tento přístup nevyužívá a nedrží se žádné konkrétní metodiky a tudíž je velice flexibilní a lehce aplikovatelný. Rizikem

tohoto přístupu je ovšem opomenutí některého z důležitých prvků systému či rizika, popřípadě implementace ne zcela adekvátního opatření na určitou hrozbu. [5]

1.6.3 Analýza rizik – kombinovaný přístup

Kombinuje analýzu rizik na hrubé úrovni s podrobným přístupem, který je aplikován na vybrané, z pohledu informační bezpečnosti kritické systémy a na zbytek doporučuje využití základního přístupu. [5]

1.6.4 Analýza rizik – podrobný přístup

Jedná se o podrobnou analýzu rizik IT systému, kdy jsou identifikována související rizika včetně odhadu jejich velikostí. Skládá se z následujících kroků:

1) Stanovení hranic revize,
2) Identifikace aktiv,
3) Ohodnocení aktiv,
4) Hodnocení hrozeb,
5) Odhad zranitelností,
6) Identifikace a určení současných i budoucích opatření,
7) Výběr ochranných opatření,
8) Odhad rizik,
9) Přijetí rizik,
10) Určení politik bezpečnosti IT systému,
11) Plán bezpečnosti IT. [5]

V praxi se nejčastěji uplatňuje využití kombinovaného přístupu vzhledem k jeho efektivitě, kdy zahrnuje základní přístup pro méně důležité systémy společně s využitím podbroného přístupu u kritických systémů. [5]

1.7 Řízení rizik

Jedná se o neustálý proces a vykonávání na sebe navazujících činností za účelem minimalizace rizik působících na systém. [4]

„Řízení rizik je komplexní proces, skládající se z několika na sebe navazujících fází a vytvářejících smyčku.“ [5] Jde tedy o proces fungující na modelu PDCA cyklu.

Obrázek 5: Smyčka procesu řízení rizik (Zdroj: 5)

V rámci ISMS je proces a doporučení k řízení rizik obsažen v normě ČSN ISO/IEC 27005:2013 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. Tato norma tak zahrnuje koncept nastavený normou ČSN ISO/IEC 27001:2014 a svojí strukturou plně podporuje implementaci bezpečnosti informací založené na přístupu řízení rizik. [5]

1.8 GDPR

V této části diplomové práce budou shrnuty základní informace, týkající se v platnost nově vcházejícího nařízení Evropské Unie (EU) – GDPR.

1.8.1 Definice GDPR

V dnešní době, kdy vlivem stále více se rozšiřujícího využívání internetu a internetu věcí, digitálních služeb a sociálních sítí hromadí společnosti kvanta osobních dat svých uživatelů za účely jejich analýzy a následného procesování, se únik a zneužití takto velkého množství dat stává stále více reálnou hrozbou, ohrožující soukromí velkého množství uživatelů.

Reakce na tuto situaci s úmyslem ochrany koncových uživatelů a jejich osobních dat ze strany EU dala vzniknout evropskému nařízení GDPR.

GDPR (celý angl. název General Data Protection Regulation) neboli Obecné nařízení o ochraně osobních údajů je novou legislativou schválenou 27.4.2016 ze strany Evropského parlamentu. GDPR vstupuje v platnost dne 25.5.2018. [12][13]

GDPR nahrazuje direktivu o ochraně osobních dat z roku 1995 (Data Protection Directive 95/46/EC) a harmonizuje zákony o ochraně a zpracování osobních údajů napříč Evropskou Unií. GDPR se vztahuje a reguluje zpracování osobních údajů fyzických osob v EU ze strany fyzické osoby, firmy nebo organizace, přičemž není podmínkou, že se sídlo organizace musí nacházet v EU, ale postačuje, aby organizace zpracovávala osobní údaje občanů žijících v EU. [12][13]

1.8.2 Klíčové pilíře GDPR

GDPR s sebou v rámci svého zavedení kromě jiného přináší několik klíčových pilířů, na jejichž základech je celé nařízení postaveno.

Hlášení úniku dat

Hlášení úniku dat, jejich ztráty nebo napadení je základním pilířem GDPR a ukládá zpracovatelům osobních dat povinnost nahlásit vzniklý únik do 72 hodin od jeho zjištění své DPA (Data Protection Authority). Zpracovatelé také musí vzniklý únik oznámit svým klientům a kontrolním orgánům bez zbytečného prodlení ihned po zjištění úniku dat. [14]

Právo na přístup

Na základě GDPR si budou moci uživatelé vyžádat od svého zpracovatele osobních údajů seznam všech údajů, které o nich zpracovatel shromažďuje společně s informacemi zdali byly jejich data již nějakým způsobem zpracovány, případně kde a za jakým účelem. Zpracovatel osobních údajů je také povinnen shromažďovaná data poskytnou žadateli v elektronické podobě zcela zdarma. [14]

Právo být zapomenut

Uživatel bude moci po svém zpracovateli osobních údajů požadovat také zapomenutí, tj. vymazání svých osobních dat z databáze a tím i zastavit případné zpracování dat. Zpracovatel je poté povinen tuto žádost posoudit a případně vyhovět či nevyhovět

požadavku na základě dalších právních norem a právního řádu dané země. [14] Například tak nebude možné požádat o výmaz z registru plátců DPH nebo jiných, podobně veřejně nutně dostupných databází.

Datová převoditelnost

GDPR umožňuje uživateli také zažádat o zaslání dříve poskytnutých dat ve strojově čitelném formátu zpět od jejich zpracovatele například pro účely jejich dalšího poskytnutí jinému zpracovateli. [14]

Soukromí „by desing“

Angl. Privacy by Design označuje koncept, kdy jsou zařízení a systémy budovány již s integrovanými bezpečnostími prvky a nejsou jim tyto prvky instalovány až dodatečně. Tento koncept je znám již řadu let, ale až s platností GDPR je pevně zanesen v rámci legislativy a bude vyžadováno jeho dodržení po výrobcích i vývojařích společně s nařízením o zpracování pouze klíčových a nezbytně nutných dat v rámci jejich systémů. [14]

Data Protection Officer (DPO)

GDPR nově zavádí funkci pověřenec pro ochranu osobních údajů (DPO), jejímž cílem je monitorování a podávání hlášení na zpracovatele dat v případě neshod s GDPR své lokální DPA. DPO může být realizován ve formě stálého zaměstnance nebo lze tuto funkci v rámci společnosti outsourcovat formou externí spolupráce. Odpovědnost za dodržení souladu s nařízením nese vždy zpracovatel údajů a nikoliv DPO. [14]

Za nedodržení souladu s nařízením GDPR hrozí zpracovatelům dat maximální pokuta až ve výši 4% ročního obratu nebo 20 000 000 EUR (podle toho, která z částek je vyšší). [14]

1.9 Emailová komunikace

V této části práce budou popsány základy emailové komunikace z důvodu nutnosti pochopení její funkčnosti vzhledem k informační bezpečnosti.

Emailová komunikace, tj. zasílání elektronických zpráv je starší než samotný internet a první emailová zpráva byla předána mezi uživateli jednoho počítače už v roku 1965 a klasický email, tak jak jej známe dnes, totiž přenos elektronické zprávy mezi dvěma zasíťovanými zařízeními byl poté uskutečněn v roce 1969, kdy byl email použit pro komunikaci na síti ARPANET v rámci experimentu, konaného Ministerstvem obrany Spojených států amerických. [10]

Emailová adresa je tvořena dvěma částmi, které jsou vzájemně odděleny znakem „@“. První část je tzv. alias a určuje konkrétního uživatele v rámci organizace/domény. Druhá část poté představuje doménové jméno (online lokaci), na kterou jsou emaily přijímány. [11]

Obsah emailové zprávy je tvořen její hlavičkou, která obsahuje předmět zprávy, adresu odesílatele, adresu příjemce a další informace o emailu jako je například datum odeslání atd. Tělo hlavičky poté obsahuje samotnou zprávu zasílanou uživatelem. [10]

V rámci emailové komunikace jsou využívány především tři typy protokolů:

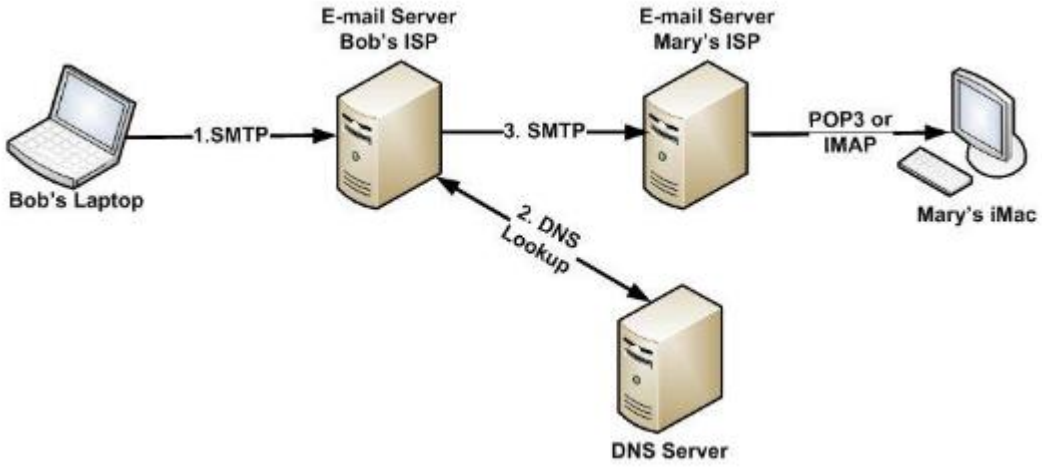
- **SMTP – Simple Mail Transfer Protocol** - protokol pro přenos emailu v prostředí internetu,
- **POP – Post Office Protocol** - protokol zabezpečující stažení emailové zprávy emailovým klientem na uživatelský počítač,
- **IMAP – Internet Mail Access Protocol** - protokol stejného typu jako POP ovšem s rozšířenými možnostmi využití jako je například tvorba složek přímo na serveru. [11]

Důležitým poznatkem je, že emailová zpráva není jakkoliv šifrována, což společně s faktem, že je během doručování v prostředí internetu transportována skrze více zařízení, přispívá k nutnosti zaměření se na prvek její bezpečnosti zvláště pak při jejím komerčním využití, kdy se skrze email mohou posílat citlivá firemní data nebo data klientů.

Mechanismus zasílání emailové pošty je poté následovný:

1) Po napsání zprávy v emailovém klientu je za pomocí SMTP protokolu zpráva předána programu Mail Transfer Agent (MTA), který na základě doménového jména adresy příjemce vyhledá příslušný Mail Exchange Server (MXS - server přijímající poštu v rámci dané domény) prostřednictvím DNS (Domain Name System).

2) DNS server odpoví MTA příslušnou adresou vyhledávaného MXS.
3) MTA odešle zprávu pomocí SMTP protokolu na MXS v doméně příjemce.
4) MXS po obdržení zprávy doručí email na základě aliasu do schránky příjemce (v případě, že se zprávu nepodaří doručit, informuje odesílatele o této skutečnosti MTA).
5) Uživatel si pomocí protokolu POP nebo IMAP stáhne doručenou poštu do počítače nebo si ji prostřednictvím svého emailového klienta prohlédne a zprávu tak zanechá uloženou na serveru. [10]



Obrázek 6: Emailová infrastruktura schéma (Zdroj: 11)

2 ANALÝZA SOUČASNÉHO STAVU

V této části své diplomové práce popíši historii analyzované společnosti, její současný stav včetně organizační struktury, její fungování, hlavní předmět podnikání a zmapuji hlavní procesy odehrávající se ve společnosti. Z oblasti bezpečnostni analyzuji její současné aplikované bezpečnostní politiky, popis používaného hardwarového vybavení včetně managementu aktiv, využívané softwarové nástroje sloužící jak k pracovním úkonům, tak i aplikované bezpečnostní prvky softwarového charakteru. Bude zde také popsána bezpečnostní situace z hlediska fyzické bezpečnosti, personální bezpečnosti společně s řízením přístupů zaměstnanců k jednotlivým druhům informací a jejich zacházení s nimi. Jelikož se jedná o společnost působící ve více evropských zemích, bude analýza zpracovaná v této části práce vztažena pouze na hlavní brněnskou centrálu společnosti, jelikož ostatní pobočky se liší jak svým pracovním zaměřením, tak i využívanými hardwarovými a softwarovými nástroji.

2.1 Popis společnosti

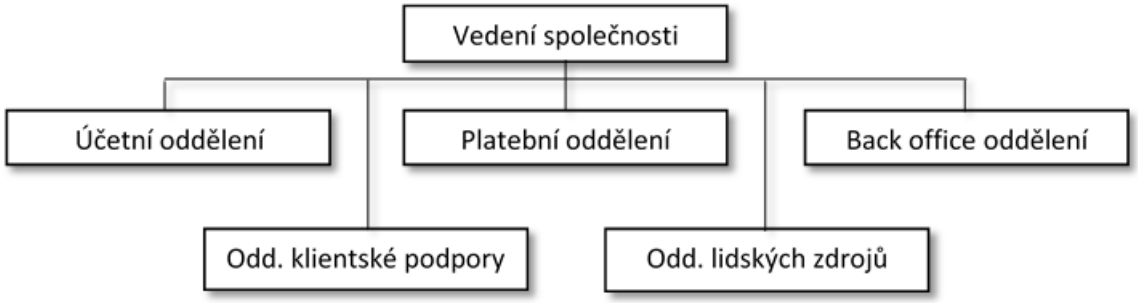
Společnost vybraná k tvorbě této diplomové práce si nepřeje být uvedena pod svým skutečným názvem vzhledem k citlivé povaze zvěřejněných informací z oblasti informační bezpečnosti. V následujících častech proto tedy bude uváděna pod názvem Obchodní s.r.o. nebo také jako „společnost“.

Společnost Obchodní s.r.o. byla založena v roce 2011 jako součást holdingu více společností s podobným předmětem podnikání – poskytování služeb spojených s obchodováním na finančních trzích. V případě Obchodní s.r.o. se jedná o poskytování služeb umožňující jejím klientům buď samostatné obchodování akciových titulů, nebo využití služeb spojených se správou jejich kapitálu třetí stranou tzv. správcem peněz. Společnost ze začátku svého působení nabízela pouze omezené množství produktů a postupným vývojem otevřela své pobočky i v dalších zemích Evropské unie, kde poskytuje své služby na mezinárodní úrovni. Centrála společnosti byla ovšem po celou dobu zachována na místě svého původního vzniku a nachází se v Brně.

Primárním předmětem podnikání Obchodní s.r.o. je, jak již bylo řečeno, poskytování služeb umožňující svým klientům obchodování na finančních trzích. K zajištění technologického zázemí jak z pohledu obchodní infrastruktury, tak i správy webu

a webových aplikací využívá služeb jedné z dalších společností působící v témže holdingu. Pro své klienty tak obstarává administrativu spojenou s otevíráním a správou klientských obchodních účtů a manipulaci s klientskými vklady v rámci přijímání vkladů či odesílání výběrů. Technologie umožňující klientům participovat na finančních trzích je poté reprezentována poskytováním obchodní platformy klientům ze strany Obchodní s.r.o.

Organizační struktura ve firmě je holokratická neboli „plochá“, kdy jednotlivý zaměstnanci pracují v rámci svých týmů, v jejichž čele stojí vždy team leader, za účelem dosažení požadovaných cílů stanovených na základě celofiremní/holdingové strategie. Vedení společnosti je sdíleno napříč celou organizací. Navzdory tomu lze poměrně snadno definovat firemní strukturu na základě rozdělení zaměstnanců do týmů – oddělení klientské podpory, platební oddělení, oddělení back office, účetní oddělení, oddělení lidských zdrojů a vedení společnosti.



Obrázek 7: Organizační schéma společnosti (Zdroj: Vlastní)

Na základě výše uvedených informací lze konstatovat, že z pohledu legislativy společnost svou povahou a nakládáním s citlivými osobními údaji svých klinetů spadá pod obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR) přijaté Evropskou unií v dubnu 2016 a platné od 25. května 2018.

2.2 Analýza hlavních podnikových procesů

Tato část práce popisuje hlavní podnikové procesy společnosti Obchodní s.r.o. společně s jejich zobrazením v podobě procesních diagramů. Cílem této části není detailní zmapování každého z procesů ve firmě, nýbrž obecný popis hlavních procesů tvořících většinu času pracovní doby zaměstnanců a procesů klíčových vzhledem k předmětu podnikání společnosti.

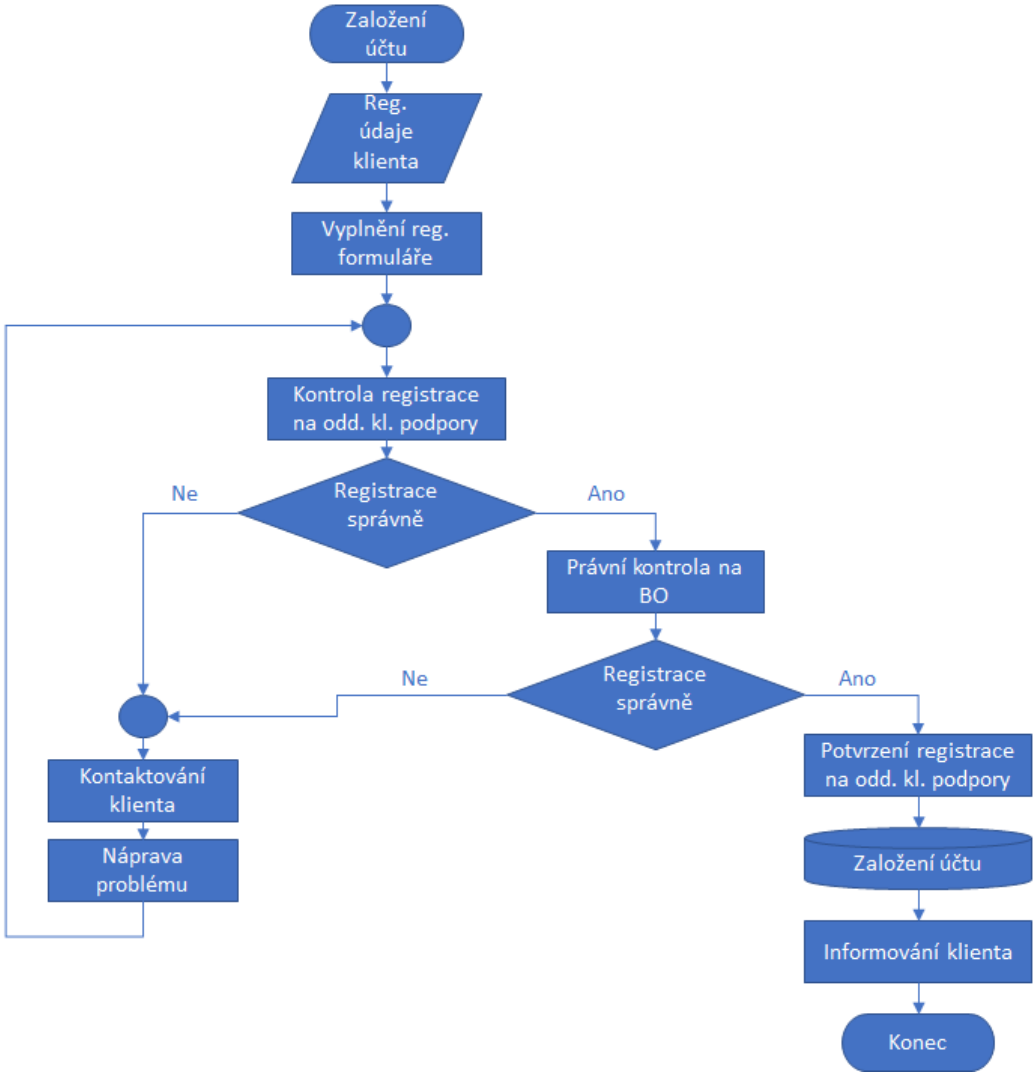
2.2.1 Založení klientského účtu

Proces založení klientského účtu začíná na straně klienta, který skrze webový formulář umístěný na registrační stránce společnosti vyplní nezbytně nutné informace potřebné k založení obchodního účtu včetně informací, jako jsou jméno a příjmení, pohlaví, datum narození a informace o své finanční situaci společně s dalšími otázkami sloužícími k zařazení klienta do jedné z rizikových skupin. Zařazení klienta na základě jeho odpovědí je vyžadováno ze zákona a tudíž je nutné doložení těchto informací po klientovi požadovat.

Následně je klient v posledním kroku registrace vyzván, aby prostřednictvím webového formuláře nahrál dokumenty potvrzující jeho totožnost a místo bydliště. Vyplněný formulář je následně předán do ticketovacího systému a zpracován pracovníkem klientské podpory, který provede kontrolu vyplněných údajů a doložených dokumentů. Pokud některá z těchto položek nesplňuje dané požadavky, je klient kontaktován prostřednictvím emailu a je po něm požadováno doložení správných informací/dokumentů.

Pokud jsou zadané údaje i dokumenty po vizuální stránce v pořádku a neobjevují se zde žádné viditelné nesrovnalosti, je registrace předána na oddělení back office k právní kontrole daného klienta (je kontrolován politický status klienta, jeho trestní bezúhonnost a případná falsifikace doložených dokumentů). Pokud jsou v tomto kroku zjištěny nesrovnalosti, je oddělení klientské podpory o konkrétní nesrovnalosti vyrozumněno a dále kontaktuje klienta v nápravě vzniklého problému.

Pokud žádné nesrovnalosti zjištěny nejsou, je schválená registrace předána zpět na oddělení klientské podpory, kde je pracovníkem po manuálním potvrzení automaticky (prostřednictvím API) založen obchodní účet (dojde k vytvoření záznamu v databázi klientů a databázi obchodních účtů), o čemž je klient následně informován prostřednictvím emailu, ve kterém nalezne všechny nezbytné informace včetně přihlašovacích údajů a odkazu ke stažení obchodní platformy.



Obrázek 8: Založení kl. účtu - schéma procesu (Zdroj: Vlastní)

2.2.2 Správa klientských financí

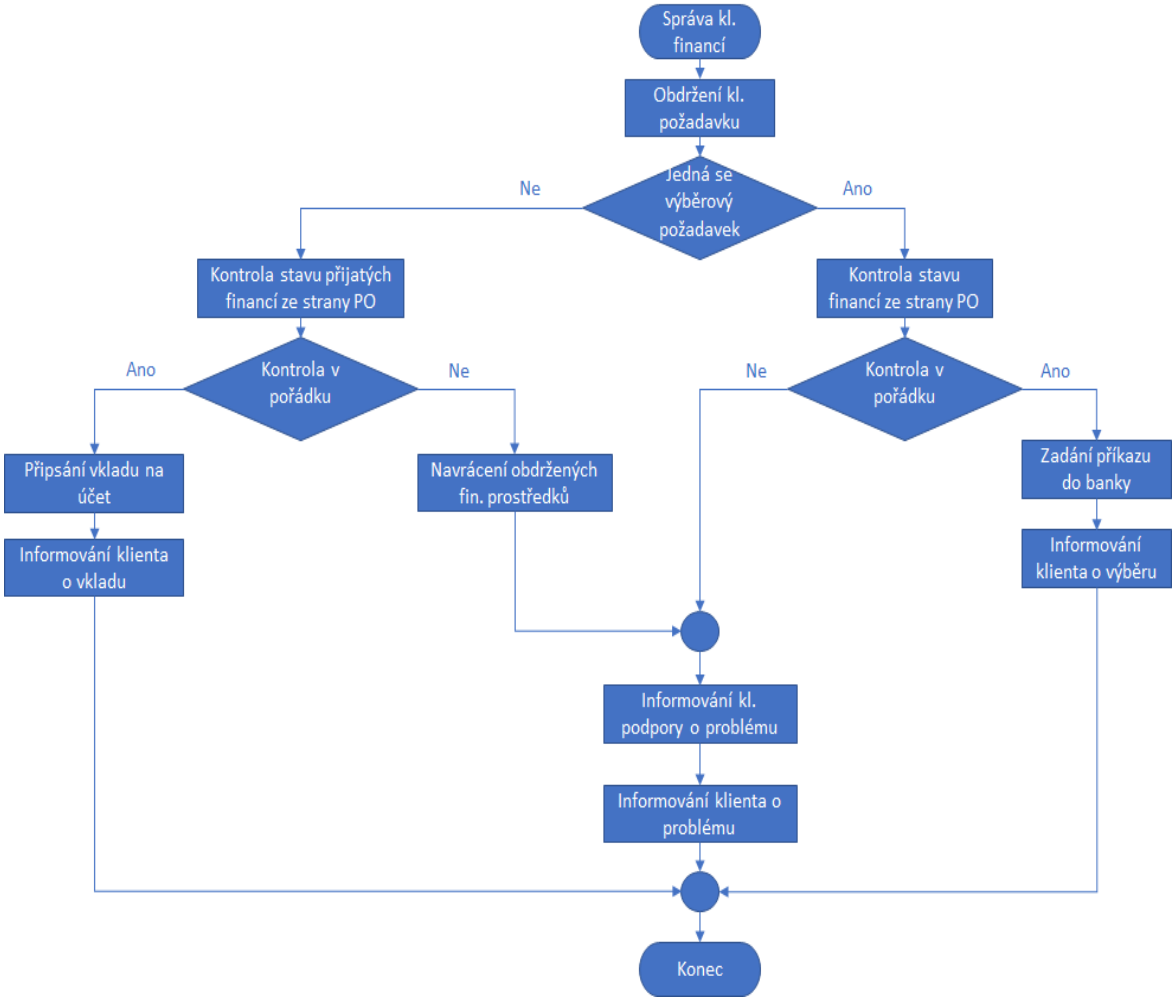
Na základě klientem podané žádosti skrze klientskou zónu je do ticketovacího systému platebního oddělení doručen požadavek buď na uskutečnění výběru, nebo vkladu finančních prostředků.

Pokud se jedná o požadavek na výběr, zkontroluje pracovník platebního oddělení, zdali má klient v databázi uveden korektní bankovní účet, popř. zdali disponuje požadovanou sumou k výběru na svém obchodním účtu. Pokud jsou všechny náležitosti v pořádku, je požadovaný výběr potvrzen a prostřednictvím specializovaného softwaru zadán příkaz k úhradě do banky ke zpracování a klient je o vyřízení zadaného požadavku automaticky informován.

V případě, že se v procesu kontroly objeví jakkékoliv nesrovnalosti, je o daném problému vyrozumněno oddělení klientské podpory, které klienta v dané věci informuje a klient je nucen si po nápravě vzniklých nesrovnalostí požádat o nový výběr.

Pokud se klientův požadavek týká zpracování jeho vkladu, kontroluje pracovník platebního oddělení, zdali byla klientem zadaná částka již obdržena v bance a zdali přišla ze schváleného obchodního účtu (účet musí být vedený na klientovo jméno). Jeli klientův vklad obdržen z jiného bankovního účtu, který není veden na klientovo jméno, je takovýto vklad zaslán zpět na účet odesílajícího a klient je o této skutečnosti informován ze strany klientské podpory.

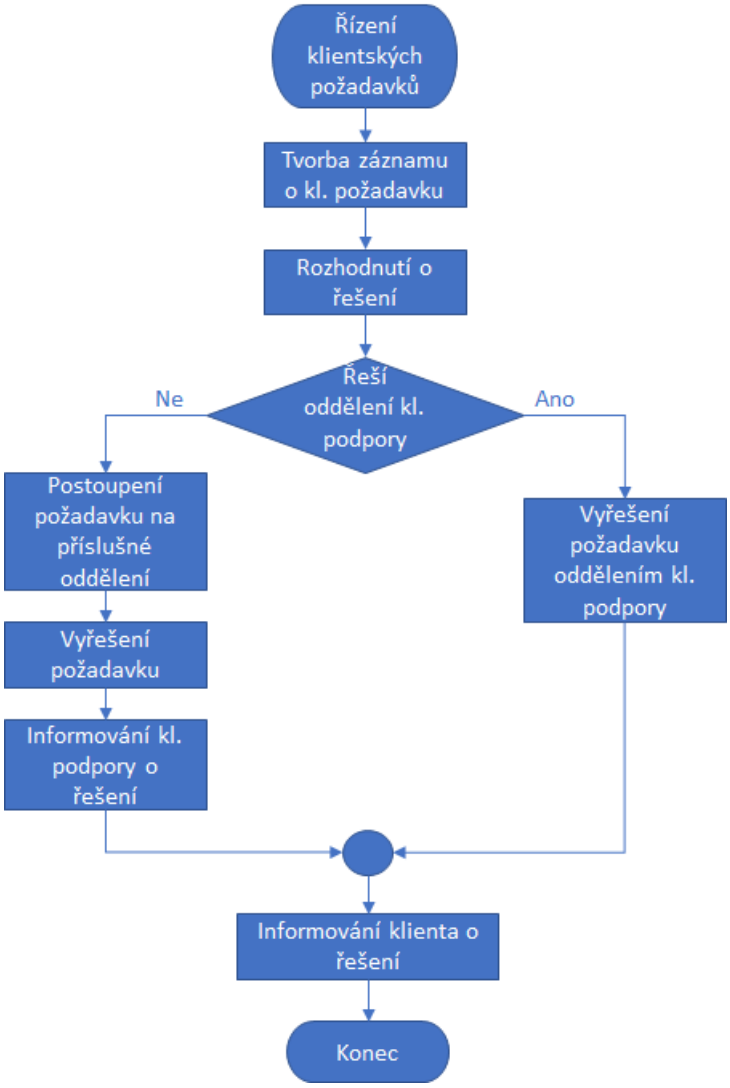
Nejsou-li během procesu kontroly vkladu zjištěny žádné nesrovnalosti, je klientovi připsán jeho vklad automaticky na obchodní účet po manuálním potvrzení ze strany pracovníka platebního oddělení a klient je o připsání vkladu automaticky informován.



Obrázek 9: Správa kl. financí - schéma procesu (Zdroj: Vlastní)

2.2.3 Řízení klientských požadavků

Řízení klientských požadavků je primární a obecný proces zpracovávaný oddělením klientské podpory. Po obdržení emailové zprávy, chatu nebo telefonického kontaktu je vytvořen v ticketovacím systému záznam s klientským požadavkem (může se jednat například o prošetření některého z ukutečněných obchodů, změnu kontaktních/osobních informací, aj.), který je následně buď zpracován samotným oddělením klientské podpory nebo je postoupen v rámci ticketovacího systému k vyřízení na jiné oddělení, které následně informuje oddělení klientské podpory o daném stavu a to poté předá zjištěné informace klientovi skrze některý z komunikačních kanálů.



Obrázek 10: Řízení kl. požadavků - schéma procesu (Zdroj: Vlastní)

2.3 Analýza IT aktiv

V této části své diplomové práce popíši nejvíce využívané hardwarové i softwarové pracovní nástroje, které jsou ve firmě využívány včetně popisu internetového připojení a ošetření jeho dostupnosti v brněnské kanceláři společnosti. Cílem této části je popsat funkčnost a přístup ke každému z klíčových softwarových nástrojů, které jsou ve firmě využívány. Za udržování aktuálního seznamu jak hardwarových, tak i softwarových aktiv včetně licenčních čísel je ve společnosti zodpovědný správce IT.

2.3.1 Analýza softwarového vybavení

Softwarové produkty, které jsou využívány zaměstnanci společnosti lze rozdělit do dvou skupin – nástroje, které je třeba instalovat na každé zařízení a cloudové služby, ke kterým lze přistupovat protřednictvím internetového prohlížeče. Společnost se snaží svým zaměstnancům umožnit co nejširší možnosti práce „odkudkoliv“ a tak lze k většině využívaných služeb přistupovat prostřednictvím internetového prohlížeče, což nuceně vede zaměstnance k tvorbě složitých přístupových údajů k těmto službám.

Aplikace Lastpass, sloužící ke správě hesel a zabezpečených poznámek, která se instaluje v podobě rozšíření do internetového prohlížeče Google Chrome poté pomáhá uživatelům se správou jejich přístupových údajů, stejně tak jako pomáhá správci s řízením uživatelských přístupů. Společnost má zakoupenou firemní licenci k této aplikaci, což ji umožňuje centrálně prostřednictvím správce řídit přístupy a možnosti sdílení přístupů napříč jednotlivými odděleními a zaměstnanci. K přihlášení do této aplikace je nutné zadat firemní emailovou adresu, přístupové heslo a prostřednictvím dvoufaktorové autentizace (buď v podobě zaslání sms a zadáním číselného kódu nebo potvrzením přístupu skrze mobilní Lastpass aplikaci) potvrdit přístup. Po přihlášení je poté uživatel schopný přihlašovat se na již uložené webové stránky, přičemž není nucen na těchto webech zadávat své přístupové údaje, jelikož je za uživatele vyplňuje automaticky Lastpass. To umožňuje uživateli nastavení odlišného, dlouhého a přitom složitého hesla pro každý z uložených webů zvlášť, kdy by si uživatel nebyl schopen za normálních okolností bez použití aplikace Lastpass tato hesla zapamatovat.

Jako emailový klient je využíváno rozhraní standardního emailového klienta Google Mail, jenž je přístupný skrze libovolný internetový prohlížeč. Společnost má i zde

zakoupenou komerční licenci pro možnost využívání firemní domény namísto původní a možnosti správy uživatelských účtů prostřednictvím správce. Přihlášení do emailového klienta je realizováno zadáním emailové adresy, hesla a ověřením skrze dvoufaktorovou autentizaci (prostřednictvím zadání kódu z mobilní aplikace Google Authenticator). Jako nadstavba pro možnost použití šifrované vnitropodnikové emailové komunikace skrze standard S/MIME je poté využíván emailový klient Thunderbird, který je navázán na jednotlivé zaměstnanecké Google Mail účty.

Dalším z využívaných programů dostupných skrze internetový prohlížeč je ticketovací systém, sloužící na zakládání záznamů týkajících se různých předmětů a jejich následné předávání mezi odděleními a provádění změn ve stavech každého z ticketů. Tento ticketovací systém sloužící i k obsluze emailové komunikace s klienty se nazývá Freshdesk a uživatelé se k němu přihlašují prostřednictvím zadání svého firemního Google účtu. Ticketovací systém je provázán s emailovým klientem a všechny záznamy z tohoto systému jsou tak ukládány ve formě emailů na předem nastaveném emailovém firemním účtu sloužícím k těmto účelům.

Jako cloudové úložiště dat pro záznamy o klientech a jejich účtech plní funkci CRM systému aplikace Podio, do níž se zaměstnanci opět přihlašují za pomocí svého firemního Google účtu. Podio je skrze firemní API rozhraní spojeno s ticketovacím systémem Freshdesk a dalšími interními systémy, což umožňuje většinu částí jednotlivých procesů plně automatizovat.

Posledním hojně využívaným nástrojem s přistupem skrze rozhraní internetového prohlížeče je firemní chatovací aplikace Slack, která slouží k rychlé komunikace uvnitř i mezi jednotlivými týmy. Datový přenos v rámci této apolikace není šifrován a z toho důvodu využívá vedení společnosti ke komunikaci o citlivých záležitostech alternativu tohoto programu a to peer-to-peer chatovací systém Semafor, jenž je postaven na platformě Java a jehož datový přenos je šifrován. Slack nabízí svým uživatelům i desktopovou aplikaci, ale většina zaměstnanců ve společnosti upřednostňuje jeho internetovou verzi.

K manipulaci s klientskými účty využívají zaměstnanci specializovaný program k tomu určený. Prostřednictvím něj jsou schopni upravovat například zůstatek na účtech a jinak

s účty manipulovat. Skupiny účtů, které zaměstnanci v tomto programu uvidí a se kterými budou moci pracovat, jsou upravitelné a přístupy k nim se dají nastavit.

Pro bezpečné ukládání citlivých klientských dokumentů, které klient poskytuje během své registrace (občanský průkaz/cestovní pas, bankovní výpis, aj.) slouží cloudové šifrované úložiště dat od společnosti Tresorit. Zaměstnanci mají nainstalovanou aplikaci Tresorit na svých počítačích a přistupují do ní přihlášením za využití přihlašovacích údajů a dvoufaktorové autentizace.

Na každém zařízení, které zaměstnanci využívají k výkonu práce (může se jednat jak o stolní PC, notebooky tak i mobilní telefony) je nainstalován antivirový program ESET Endpoint Security od společnosti ESET, který umožňuje kromě klasické funkce antiviru také v případě vzniku bezpečnostního incidentu na dálku dané zařízení uzamknout nebo nastavit pravidla pro procházení internetových stránek.

Na přenosných zařízeních určených k práci jako jsou notebooky a mobilní telefony, které se k internetu připojují na veřejných či jinak nedůvěryhodných sítích je nainstalován program Encrypt.me sloužící pro vytvoření šifrovaného VPN spojení. Tento program jsou zaměstnanci nuceni využívat vždy, když se připojují k internetu na jiné než firemní zabezpečené síti.

2.3.2 Internetové připojení kanceláře

Jednotlivé pracovní stolní PC včetně dalších síťových zařízení jsou zasíťovány a zapojeny do rozvaděče, umístěného v oddělené místnosti s omezeným přístupem. Připojení jednotlivých zařízení k rozvaděči je realizováno metalickou kabeláží, kdežto samotný rozvaděč je poté napojen přímo k páteřní síti celé budovy, realizované na optické kabeláži. Internetové připojení kanceláře je poskytováno od společnosti Global communications s.r.o. s parametry 400Mbit/s download a 200Mbit/s upload. WiFi síť je v kanceláři řešena pomocí dvou access pointů, umístěných vhodně tak, aby byla WiFi signálem pokryta plocha celé kanceláře.

2.3.3 Analýza hardwarových aktiv

Zaměstnanci společnosti využívají ke své práci firemní stolní počítače značky Dell, přičemž je každému ze zaměstnanců umožněno libovolně konfigurovat hardwarové

vybavení svého PC vzhledem k výkonu jeho profese a v rámci předem stanoveného rozpočtu. Společnost má také k dispozici notebooky značky Lenovo E470 a jeden MacBook Air. Tato zařízení může společnost v případě potřeby zapůjčit svým zaměstnancům, kteří potřebují pracovat vzdáleně. Většina zaměstnanců využívá ke své práci dvou monitorů. Užívané monitory jsou značky Iiyama a velikosti 24 palců.

V serverové místnosti je poté umístěný 19ti palcový rozvaděč s možností osazení až 42U. Rozvaděč je osazen routerem Cisco RV325, dvěma switchi Cisco SG220-50 o velikosti 1U, VPN serverem, NAS úložištěm Synology RS816, kamerovým systémem a třemi modulárními patch panely Digitus. O chlazení celého rozvaděče se poté starají tři ventilátory a náhradní výkon v případě výpadku elektrického proudu zajišťuje jedna UPS. Rozvaděč se nyní jeví jako naddimenzovaný současnému využití, nicméně s velmi rychle rostoucím počtem zaměstnanců se zvětšují i požadavky na počet přípojných míst, na které chce být společnost připravena již nyní.

Z patch panelů jsou linky taženy po metalické kabeláži kategorie 5e a jsou zakončeny v zásuvkách o různém počtu portů (2 nebo 3 dle potřeby) typu RJ-45. Kabeláž je v rámci kanceláře tažena podlahovým systémem a v jednotlivých místností poté přechází do plastových žlabů.

2.4 Analýza současného stavu bezpečnosti podniku

V této části práce budou analyzován současný stav bezpečnosti podniku.

2.4.1 Aplikované bezpečnostní politiky podniku

Informační bezpečnost je nyní ve společnosti řešena pomocí několika vydaných a platných směrnic, které zaměstnancům nařizují a předepisují definované způsoby, jakými lze mohou či nemohou zaměstnanci nakládat s informačními aktivy společnosti.

První ze směrnic definuje způsoby používání IT zařízení, jakými jsou například firemní stolní počítače nebo osobní notebooky, které si zaměstnanci přinesou z domu a hodlají je využívat v pracovním prostředí. Jsou v ní také uvedena pravidla pro bezpečné využívání bezpečnostních prvků v případě přístupu k firemním systémům. Směrnice nařizuje kromě jiného například povinnost uzamknout počítač při odchodu zaměstnance od pracovního místa, použití VPN při připojování k jakékoliv jiné než firemní síti, zákaz uchovávání

hesel v podobě zápisů na běžně dostupných místech, nutnost nastavení dvoufaktorové autentizace při přístupu k vybraným firemním systémům a jiné.

Druhá ze směrnic definuje způsob a obsah vstupního školení zaměstnanců týkající se práce s firemními informačními systémy a nakládání s firemními informacemi. Obsahem školení je kromě všeobecných základů bezpečnosti v prostředí internetu a využívání firemních zařízení také i poučení o striktním využívání pouze firemního softwaru, zákazu vkládání přenositelných médií do pracovních zařízení nebo způsobu, jak se zachovat v případě obdržení podezřelého souboru v emailové schránce, přičemž tato část je důkladněji probírána hlavně se zaměstnanci oddělení podpory, kteří se s případnou hrozbou útoku v podobě obdržení infikovaného dokumentu mohou setkat nejčastěji. Školení je zakončeno písemným testem, který je poté vyhodnocen školícím pracovníkem (zaměstnanec IT) a v případě nedosažení požadovaného minimálního množství bodů je daný zaměstnanec nucen test opakovat.

Další ze zavedených směrnic týkající se bezpečnosti je směrnice upravující a zavazující zaměstnance uchovávat důvěrné, citlivé informace jak o společnosti, jejích obchodních tajemstvích, tak i klientech v tajnosti. Tato směrnice také určuje, jakým způsobem bude dodržování výše zmíněných požadavků vynucováno a definuje případné postihy zaměstnanců v případě jejich nedodržení.

2.4.2 Fyzické zabezpečení společnosti

Společnost sídlí v centru Brna, přičemž v jedné z komerčních budov má v současnosti pronajaté kancelářské prostory na rozloze celých dvou pater dané budovy. Patra jsou navzájem průchozí a tak není nutné opouštět kancelářské prostory při potřebě přechodu z jednoho patra do druhého. Prostory budovy, kde společnost sídlí, obývají další tři společnosti, přičemž možnost průchodu z jedné firmy do druhé není možná.

Do budovy vedou dvě přístupové cesty, kdy jedna z nich je hlavním vchodem z ulice a další ze dvora, kam nemá veřejnost přístup. V obou případech je nutné projít kolem recepce s ostrahou. Budova má jedno schodiště a jeden výtah.

Zabezpečení budovy je zajištěno kamerovým systémem, kdy kamery snímají oba vchody do budovy. Alarm není v rámci chodeb budov instalován. I když se budova zamyká každý den ve 20:00, mají do ní zaměstnanci firem, sídlících v budově, neomezený přístup

a disponují klíči od budovy. Požární detektory jsou umístěny jak na chodbách, schodišti tak i ve výtahu a na každém patře budovy jsou umístěny hasicí přístroje.

Vchod do samotné kanceláře je poté možný na každém ze dvou pater. Vchody kanceláře jsou zajištěny uzamykatelnými dveřmi a kódovým systémem, pomocí něhož lze zajistit vnitřní prostory kanceláře skrze alarmový systém, jenž má pohybová čidla rozmístěna v každé z místností nacházejících se v prostorách kanceláře. Zaměstnanci jsou tak vybaveni klíči od budovy, vstupních dveří kanceláře a osobním čipem, pomocí kterého mohou alarmový systém ovládat.

Vstupy do kanceláře jsou také zabezpečeny kamerovým systémem. Uvnitř kanceláře se poté nachází vstup na terasu, která je také zabezpečena kamerovým systémem stejně tak jako přístup do účetního oddělení.

Účetní oddělení je vzhledem k citlivé povaze dokumentů, jenž jsou na daném oddělení zpracovávány vícenásobně zabezpečeno oproti přístupům do jiných oddělení. Každý zaměstnanec účetního oddělení je povinen vstupní dveře uzavírat v případě, že prostory oddělení opouští a nikdo jiný se již v oddělení nenachází. Přístup do tohoto oddělení je zabezpečen kódovým zámkem, který se dá odemknout pouze čipem některého ze zaměstnanců oddělení a další osoby tak nejsou schopny dveře otevřít. Účetní oddělení je také vybaveno speciálním, na míru dělaným trezorem, sloužícím k uchovávání citlivých dokumentů.

Místnost s rozvaděčem je umístěna tak, aby v jejím okolí nebylo žádné rozvodové vodovodní potrubí, a přístup do ní je také řízen prostřednictvím kódového zámku.

V prostorách celé kanceláře jsou poté umístěny požární detektory, jejichž pravidelné zkoušení a údržbu zajišťuje správa budovy. Hasicí přístroje jsou rovněž umístěny na každém patře kanceláře s dobrým přístupem. Kanceláře jsou klimatizovány centrální klimatizací, ke které je přístup omezen a zabezpečuje jej taktéž správa budovy.

2.4.3 Lidské zdroje a řízení přístupů

Zaměstnanci jsou do podniku nabíráni na základě tříkolového výběrového řízení, kterým musí všichni uchazeči bezpodmínečně projít. V jednotlivých kolech pohovoru musí každý z uchazečů o zaměstnání prokázat své kvality a to vždy za přítomnosti zaměstnance oddělení lidských zdrojů a jednoho dalšího zaměstnance – nejčastěji se jedná o leadera

týmu, do kterého by byl daný uchazeč zařazen v případě úspěšného absolvování přijímacího řízení. V rámci druhého kola pohovoru je uchazeč také podroben testu v podobě vypracování případové studie a to přímo v prostorách kanceláře. Uchazeči také může být umožněno vypracování případové studie doma a to většinou v případě složitějšího a časově náročnějšího zadání (zejména při programátorských úlohách).

Při nástupu do zaměstnání je uchazeč nucen porobit se lékařské kontrole, o jejímž úspěšném absolvování je prostřednictvím lékařského potvrzení vyrozuměno oddělení lidských zdrojů. Při nástupu každého nového zaměstnance je s každým uchazečem také podepsána dohoda o mlčenlivosti. Další povinností každého z nově přijatých uchazečů je nutnost absolvovat školení týkající se BOZP a informační bezpečnosti. Školení ohledně fungování společnosti, případně specifická školení pro uchazečovu pozici jsou poté řízena již ze strany leadera týmu a svým obsahem se liší podle každé pozice a místa (oddělení) jejího výkonu.

Ve službě Active Directory je poté novému zaměstnanci IT správcem vytvořen přístup, pomocí něhož se zaměstnanec přihlašuje k firemnímu počítači či notebooku a také jsou každému z takto vytvořených přístupů udělena odpovídající přístupová práva, odvíjející se od pracovní pozice, kterou daný zaměstnanec vykonává.

Správa hesel a přístupových údajů včetně nastavení přístupových práv v rámci jednotlivých služeb je prováděno centrálně správcem IT. Správce IT je také zodpovědný za korektní distribuci nových, v případě nutnosti úpravy poté také modifikovaných přístupových údajů mezi zaměstnanci.

Po ukončení svého pracovního závazku je každý zaměstnanec nucen odevzdat svůj přístupový čip i s klíči od budovy na oddělení lidských zdrojů a správcem IT mu je neprodleně odebrán přístup do všech firemních systémů. Zaměstnanec je poté nucen dodržovat obchodní tajemství, k němuž se zavázal podpisem dohody o mlčenlivosti při nástupu na danou pracovní pozici.

2.5 Zhodnocení současného stavu bezpečnosti podniku

Na základě analýzy současného stavu bezpečnosti podniku lze vyvodit následující závěry.

Společnost využívá množství programového vybavení a služeb prostřednictvím cloudového řešení tak, aby zaměstnancům umožnila pracovat na dálku. Hardwarové vybavení jak kancelářské (PC zaměstnanců) tak i síťové (včetně hardwaru umístěného v serverové místnosti) je dimenzováno tak, aby odpovídalo potřebám společnosti a každého ze zaměstnanců.

Společnost v současné době řídí informační bezpečnost prostřednictvím několika vydaných směrnic upravujících povinnosti zaměstnanců, týkajících se manipulace s informačními aktivy společnosti a s jejich nakládáním. Fyzická bezpečnost zázemí společnosti je díky sídlu v komerční budově v centru města na plně dostačující úrovni. Řízení lidských zdrojů a s tím spjaté řízení přístupů jednotlivých zaměstnanců je spravováno centrálně prostřednictvím správce IT. Samotné nakládání s přístupovými údaji ze strany zaměstnanců je poté řešeno pomocí specializovaného softwaru.

Hlavní podnikové procesy jsou společností zmapovány, nicméně chybí provedení celkové analýzy rizik a její vyhodnocení v kontextu informační bezpečnosti.

Provedení analýzy rizik a její vyhodnocení včetně návrhu bezpečnostních opatření na nejvíce problematické hrozby bude náplní další části diplomové práce.

3 NÁVRH VLASTNÍHO ŘEŠENÍ

Tato část diplomové práce je zaměřena na návrh vlastního řešení pro vybranou společnost. V její první části bude provedena analýza rizik na základě identifikovaných aktiv a hrozeb a jejich ohodnocení. Z provedené analýzy rizik bude poté vybrán nejkritičtější problém, potenciálně ohrožující informační bezpečnost ve společnosti. Ve druhé části pak bude na vybraný problém navrhnuto bezpečnostní opatření k akvizici na základě výběru z několika možných řešení včetně popisu jeho funkčnosti a postupu jeho zavedení do praxe. Ve třetí části Zhodnocení zavedeného opatření bude poté provedeno shrnutí a zhodnocení navrhovaného bezpečnostního opatření jak z hlediska ekonomického, tak i časového, kde bude vyměřeno, za jak dlouho dobu bude moci společnost vybrané opatření začít používat v reálném provozu a jaké náklady budou s provozem daného opatření spojeny, rozhodne-li se společnost pro jeho akvizici.

3.1 Analýza rizik

V rámci analýzy rizik bude provedena identifikace z pohledu informační bezpečnosti relevantních aktiv společnosti a jejich ohodnocení na základě potřeb jejich dostupnosti, integrity a důvěrnosti. Identifikované hrozby včetně pravděpodobnosti jejich výskytu budou společně s aktivy shrnuty v matici zranitelnosti, na základě které bude poté vypracována matice rizik, pomocí které bude zjištěna nejrizikovější hrozba. Analýza rizik vychází z informací zjištěných při analýze současného stavu a také využívá dodatečné informace, které byly zjištěny během konzultací s managementem společnosti a zainteresovanými stranami.

3.1.1 Identifikace a ohodnocení aktiv

Při identifikaci aktiv byl brán zřetel především na samotný výběr aktiva a jeho možné působení v rámci informační bezpečnosti. Z tohoto důvodu nebyla vybrána všechna aktiva společnosti, nýbrž pouze ta, jejichž věcný obsah je s informační bezpečností alespoň částečně spjat. Výběr aktiv shrnuje následující tabulka.

Tabulka 1: Identifikace aktiv (Zdroj: Vlastní)

Kategorie aktiv	Aktiva	Umístění
Data	Firemní data	Kancelář
	Zaměstnanecká data	Kancelář
	Zdrojové kódy	Cloud
	Zálohy dat	Cloud/kancelář
	Klientská data	Kancelář
Hardwarové vybavení	Pracovní stanice	Kancelář
	Notebooky	Zaměstnanci
	Mobilní telefony	Zaměstnanci
	Tiskárny	Kancelář
	Kamerový systém	Kancelář
Softwarové vybavení	Operační systémy	Kancelář/zaměstnanci
	Emailová služba	Cloud
	Cloudové služby	Cloud
	SW pro správu kl. účtů	Kancelář/zaměstnanci
	Bezpečnostní SW (antivir. programy, VPN)	Kancelář/zaměstnanci
Síťová aktiva	Síťová zařízení	Kancelář
	Kabeláž	Kancelář
Služby	Internetové připojení	Kancelář/budova
	Rozvod elektrické energie	Kancelář/budova
	Údržba, servis	Kancelář/budova

Jako škála pro ohodnocení jednotlivých aktiv byla zvolena stupnice od „1“ do „5“, kdy nízké hodnocení značí nízkou hodnotu aktiva z pohledu informační bezpečnosti a vysoké hodnocení udává vysokou hodnotu aktiva.

Tabulka 2: Škála hodnocení aktiv (Zdroj: Vlastní)

Hodnota aktiva	Úroveň rizika	Dopad v případě narušení aktiva
1	bezvýznamná	Bez dopadu
2	akceptovatelná	Zanedbatelný dopad
3	nízká	Vznik finančních ztrát
4	nežádoucí	Velké finanční ztráty a další dopady
5	nepřijatelná	Existenční problémy

Celková hodnota aktiva je poté dána následujícím vztahem, který bere v potaz ohodnocení aktiva z pohledu narušení každého ze tří prvků informační bezpečnosti, tj. dostupnosti, integrity a důvěrnosti.

$$\boldsymbol{hodnota\ aktiva} = \frac{\boldsymbol{dostupnost} + \boldsymbol{integrita} + \boldsymbol{důvěrnost}}{\mathbf{3}}$$

Samotné ohodnocení aktiv poté shrnuje následující tabulka.

Tabulka 3: Hodnocení aktiv (Zdroj: Vlastní)

Kategorie aktiv	Aktiva	Dostupnost	Integrita	Důvěrnost	Hodnota aktiva
Data	Firemní data	4	4	5	4
	Zaměstnanecká data	3	5	5	4
	Zdrojové kódy	2	3	4	3
	Zálohy dat	2	3	3	3
	Klientská data	5	5	5	5
Hardwarové vybavení	Pracovní stanice	3	4	4	4
	Notebooky	4	4	5	4
	Mobilní telefony	4	3	5	4
	Tiskárny	2	2	1	2
	Kamerový systém	1	3	3	2
Softwarové vybavení	Operační systémy	3	4	3	3
	Emailová služba	5	5	5	5
	Cloudové služby	5	5	4	5
	SW pro správu kl. účtů	4	3	3	3
	Bezpečnostní SW	2	4	3	3
Síťová aktiva	Síťová zařízení	4	4	3	4
	Kabeláž	4	4	3	4
Služby	Internetové připojení	4	4	5	4
	Rozvod el. energie	3	1	2	2
	Údržba, servis	2	1	1	1

3.1.2 Identifikace hrozeb

Pro vytvoření komplexní analýzy rizik je zapotřebí také identifikovat potenciální hrozby, které mohou působit na identifikovná aktiva a zapříčinit tak vznik bezpečnostního incidentu. Při identifikaci potenciálních hrozeb byl brán zřetel, stejně jako v případě identifikace aktiv, především na hrozby s co největší pravděpodobností reálného výskytu. Identifikace hrozeb je založena a vychází z normy ČSN ISO/IEC 27005:2013. Identifikované hrozby jsou sepsány v následující tabulce.

Tabulka 4: Identifikace hrozeb (Zdroj: Vlastní)

Kategorie hrozeb	Hrozby
Fyzické	Požár
	Poškození vodou
	Znečištění
	Fyzické zničení
Technické	Selhání HW vybavení
	Selhání SW vybavení
	Chybné fungování
	Selhání údržby
Informační	Únik interních informací
	Odcizení podnikových dat
	Odcizení klientských dat
	Vyzrazení
	Napadení malwarem
	Vzdálená špionáž
	Falšování pomocí SW
	Data pocházející z nedův. zdrojů
	Odcizení vybavení
Nedostupnost služeb	Výpadek el. připojení
	Výpadek internetového připojení
Neoprávněné činnosti	Neoprávněné použití zař.
	Poškození dat
	Chyba v používání dat
	Zneužití oprávnění
	Falšování práv

Pro určení pravděpodobnosti výskytu dané hrozby jsem zvolil opět škálu hodnocení od „1“ do „5“, přičemž jednotlivé hodnoty na stupnici odpovídají pravděpodobnostem, uvedeným v tabulce pravděpodobnosti výskytu hrozeb.

Tabulka 5: Škála pravděpodobnosti výskytu hrozeb (Zdroj: Vlastní)

Hodnota	Pravděpodobnost výskytu
1	velmi nízká
2	nízká
3	střední
4	vysoká
5	velmi vysoká

V níže uvedené tabulce je poté uveden soupis všech relevatních identifikovaných hrozeb včetně přiřazených pravděpodobností jejich výskytů.

Tabulka 6: Pravděpodobnost výskytu hrozeb (Zdroj: Vlastní)

Kategorie hrozeb	Hrozby	Hodnota
Fyzické	Požár	2
	Poškození vodou	1
	Znečištění	2
	Fyzické zničení	3
Technické	Selhání HW vybavení	4
	Selhání SW vybavení	3
	Chybné fungování	2
	Selhání údržby	2
Informační	Únik interních informací	3
	Odcizení podnikových dat	2
	Odcizení klientských dat	4
	Vyzrazení	3
	Napadení malwarem	3
	Vzdálená špionáž	2
	Falšování pomocí SW	2
	Data pocházející z nedův. zdrojů	3
	Odcizení vybavení	2
Nedostupnost služeb	Výpadek el. připojení	2
	Výpadek internetového připojení	4
Neoprávněné činnosti	Neoprávněné použití zař.	2
	Poškození dat	3
	Chyba v používání dat	3
	Zneužití oprávnění	4
	Falšování práv	2

Na základě analýz, během kterých byla identifikována a ohodnocena jak aktiva společnosti, tak i hrozby, které na ně působí, byla sestrojena matice zranitelnosti. Matice zranitelnosti reprezentuje zranitelnost každého z identifikovaných aktiv vůči identifikovaným hrozbám. V matici zranitelnosti je každému průniku aktiva s hrozbou přiřazena číselná hodnota na škále od „1“ do „5“, přičemž čím je hodnota vyšší, tím je zranitelnost daného aktiva vůči konkrétní hrozbě vyšší. Číselné ohodnocení každé ze zranitelností bylo provedeno na základě subjektivního určení autora práce.

Tabulka 7: Matice zranitelnosti (Zdroj: Vlastní)

Matice zranitelnosti (V)		Aktiva	Firemní data	Zaměstnanecká data	Zdrojové kódy	Zálohy dat	Klientská data	Pracovní stanice	Notebooky	Mobilní telefony	Tiskárny	Kamerový systém	Operační systémy	Emailová služba	Cloudové služby	SW pro správu kl. účtů	Bezpečnostní SW	Síťová zařízení	Kabeláž	Internetové připojení	Rozvod elektrické en.	Údržba, servis
		A	4	4	3	3	5	4	4	4	2	2	3	5	5	3	3	4	4	4	2	1
Hrozby	**T**																					
Požár	2		1	1		3		3	3	1	3	2						3	4		4	
Poškození vodou	1		1	1				4	4	4	3	2						2	3		3	
Znečištění	2							3	4	4	3	3						3	4		3	
Fyzické zničení	3		3	3				4	4	4	3	3						4	4		3	
Selhání HW vybavení	4		2	2	3	3	3	4	4	4	4	4	3			3		4	2	3		
Selhání SW vybavení	3		3	3	3	3	4	3	3	3	1	2	4	4	4	4	4	3				
Chybné fungování	2					3		4	4	4	4	3	2	2	2	2	2	3	2	2	1	
Selhání údržby	2					4		3	3	4	4	2	2					4	3	3	3	4
Únik interních informací	3		4	4	3	4	4							3	3	4						
Odcizení pod. dat	2		5	2	3	3	4	2	3	4				4	4	4						
Odcizení kl. dat	4					3	4	3	3	3				5	3	4						
Vyzrazení	3		4	3	3	2	4															
Napadení malwarem	3		3	3	2	3	4	4	4	4	2	2	4	2	2	2	1	3				
Vzdálená špionáž	2		2	2	3	3	2	3	2	4	1	4	3	2	2	2		4				
Falšování pomocí SW	2		2	2	3	4	4															
Data z nedův. zdrojů	3		2	3	2	2	4	2	2	4								2				
Odcizení vybavení	2							4	4	5	3	2						4	3			
Výpadek el. připojení	2							4	3	2	3	4						4	3	4	4	
Výpadek int. připojení	4					3		4	3	2	3	2		4	4	4	2	3		4		
Neoprávněné použití zař.	2							3	4	4	3	2						4	3		4	
Poškození dat	3		4	4	3	3	3						3	2	2	2	1					
Chyba v používání dat	3		2	4	3	4	2	3	3	4	1			3	3	2						
Zneužití oprávnění	4		3	3	3	4	4				3	2		3	2	4		3		4		
Falšování práv	2							2	2	3		2	3	3	4	4						

3.1.3 Míra rizik

Pro určení celkové míry rizika byla vypracována matice rizik, která celkovou míru rizika tj. působení určité hrozby na dané aktivum určuje na základě následujícího vzorce.

$$R = A \; x \; T \; x \; V$$

- R = počítaná míra rizika
- A = hodnota aktiva vypočítána na základě analýzy aktiv
- T = pravděpodobnost výskytu dané hrozby získaná analýzou hrozeb
- V = určená míra zranitelnosti vycházející z matice zranitelnosti

Škála, na základě které budou poté vyhodnoceny jednotlivé celkové míry rizik, je uvedena v následující tabulce.

Tabulka 8: Škála míry rizik (Zdroj: Vlastní)

Hodnota míry rizika	Míra rizika	Dopad
0 - 24	bezvýznamná	Bez dopadu
25 - 49	akceptovatelná	Zanedbatelný dopad
50 - 74	nízká	Vznik finančních ztrát
75 - 99	nežádoucí	Velké finanční ztráty a další dopady
100 a více	nepřijatelná	Existenční problémy

Maximální možná velikost míry rizika je 125 a vychází z předpokladu, že hodnota aktiva byla stanovena na hodnotu 5, pravděpodobnost se kterou na aktivum působí hrozba je také na hodnotě 5 a stejně tak i zranitelnost, přiřazená k danému aktivu a hrozbě odpovídá hodnotě 5. Matice rizik slouží především jako informativní výstup, který nám na základě získané míry rizika udává, jaká rizika je v rámci zavádění informační bezpečnosti vhodné prioritizovat a postarat se o jejich ošetření, jelikož jejich případné naplnění by mělo závažné dopady na chod společnosti a naopak, která rizika je možné řešit později nebo je zcela akceptovat.

Tabulka 9: Matice rizik (Zdroj: Vlastní)

Matice rizik (R)		Aktiva	Firemní data	Zaměstnanecká data	Zdrojové kódy	Zálohy dat	Klientská data	Pracovní stanice	Notebooky	Mobilní telefony	Tiskárny	Kamerový systém	Operační systémy	Emailová služba	Cloudové služby	SW pro správu kl. účtů	Bezpečnostní SW	Síťová zařízení	Kabeláž	Internetové připojení	Rozvod elektrické en.	Údržba, servis
		A	4	4	3	3	5	4	4	4	2	2	3	5	5	3	3	4	4	4	2	1
Hrozby	**T**																					
Požár	2		8	8		18		24	24	8	12	8						24	32		16	
Poškození vodou	1		4	4				16	16	16	6	4						8	12		6	
Znečištění	2							24	32	32	12	12						24	32		12	
Fyzické zničení	3		36	36				48	48	48	18	18						48	48		18	
Selhání HW vybavení	4		32	32	36	36	60	64	64	64	32	32	36			36		64	32	48		
Selhání SW vybavení	3		36	36	27	27	60	36	36	36	6	12	36	60	60	36	36	36				
Chybné fungování	2					18		32	32	32	16	12	12	20	20	12	12	24	16	16	4	
Selhání údržby	2					24		24	24	32	16	8	12					32	24	24	12	8
Únik interních informací	3		48	48	27	36	60							45	45	36						
Odcizení pod. dat	2		40	16	18	18	40	16	24	32				40	40	24						
Odcizení kl. dat	4					36	80	48	48	48				100	60	48						
Vyzrazení	3		48	36	27	18	60															
Napadení malwarem	3		36	36	18	27	60	48	48	48	12	12	36	30	30	18	9	36				
Vzdálená špionáž	2		16	16	18	18	20	24	16	32	4	16	18	20	20	12		32				
Falšování pomocí SW	2		16	16	18	24	40															
Data z nedův. zdrojů	3		24	36	18	18	60	24	24	48								24				
Odcizení vybavení	2							32	32	40	12	8						32	24			
Výpadek el. připojení	2							32	24	16	12	16						32	24	32	16	
Výpadek int. připojení	4					36		64	48	32	24	16		80	80	48	24	48		64		
Neoprávněné použití zař.	2							24	32	32	12	8						32	24		16	
Poškození dat	3		48	48	27	27	45						27	30	30	18	9					
Chyba v používání dat	3		24	48	27	36	30	36	36	48	6			45	45	18						
Zneužití oprávnění	4		48	48	36	48	80				24	16		60	40	48		48		64		
Falšování práv	2							16	16	24		8	18	30	40	24						

3.1.4 Vyhodnocení analýzy rizik

Na základě identifikace a ohodnocení informačních aktiv společnosti a potenciálních hrozeb, které na identifikovaná aktiva mohou působit, byla sestrojena matice zranitelnosti. Na základě sestavené matice zranitelnosti byla poté vyhotovena matice rizik, ze které vyplývá, že mezi nejcennější aktiva společnosti patří klientská data, emailová služba a cloudové služby.

Bezpečnost klientských dat je z pohledu informační bezpečnosti vnímána velice vážně, jelikož klient je nucen pro založení obchodního účtu poskytnout společnosti všechny

potřebné dokumenty (tento požadavek vychází z regulatorních předpisů), které obsahují velmi citlivá osobní data o daném klientovi.

Cloudové služby jsou ceněny především proto, že většina pracovních nástrojů, se kterými zaměstnanci pracují, funguje v rámci cloudu a při jejich případné nefunkčnosti je většina procesů ve firmě tímto výpadkem zasažena a procesy musí být pozastaveny, což negativně ovlivňuje nabízené služby a reputaci společnosti.

Emailová služba vyšla jako třetí cenné aktivum a to z toho důvodu, že prostřednictvím ní probíhá drtivá většina komunikace mezi zaměstnanci a také mezi společností a jejími klienty. Prostřednictvím emailové služby se také přistupuje do většiny využívaných cloudových služeb.

Na výše uvedená aktiva působí nejzávažněji především tyto dvě hrozby – odcizení klientských dat a výpadek a internetového připojení. Při odcizení klientských dat by společnost čelila bezpochyby žalobě ze strany klientů, čímž by razantně utrpělo dobré jméno společnosti a na základě nového evropského nařízení GDPR by mohla být společnosti vyměřena pokuta o takové výši, jenž by mohla být pro společnost likvidační. V případě vypadku internetového připojení se stává většina služeb nedostupných a proto je tato hrozba druhou největší.

Z matice rizik lze vyčíst, že největší hrozbu představuje odcizení klientských dat v emailové službě. Proces doposílání nových citlivých klientských dokumentů v případě jejich zamítnutí během procesu zakládání obchodního účtu není ze strany společnosti prozatím jakkoliv zabezpečen. Dochází pak k tomu, že je klient vyzván, aby prostřednictvím emailové komunikace zaslal společnosti nový požadovaný dokument ve formě běžné emailové přílohy. Jelikož není emailová komunikace jakkoliv chráněna, hrozí zde v případku zachycení takovéto zprávy, která obsahuje citlivá klientská data, třetí stranou možné zneužití takovýmto způsobem zasílaných klientských dat.

Další část práce se tak bude zabývat volbou vhodného bezpečnostního opatření ve formě akvizice některé ze služeb, které nějakou formu zabezpečení emailové komunikace na úrovni mezi společností a klientem nabízejí.

3.2 Zavedení bezpečnostního opatření

V této části diplomové práce bude popsán návrh vhodných řešení k akvizici pro zabezpečení emailové komunikace (především přenášených dokumentů) mezi společností a klientem, kdy požadavek na zabezpečení tohoto procesu vyvstal z provedené analýzy rizik. Jednotlivá navrhovaná řešení zde budou popsána z pohledu obecného fungování a procesu jejich případného využívání po zavedení, včetně časové náročnosti implementace a nákladů s tím spojených. Řešeni zde budou poté srovnána a na základě tohoto srovnání bude doporučeno jedno řešení vhodné k akvizici včetně zdůvodnění jeho výběru a popsání procesu implementace.

3.2.1 Akceptace rizik

Vzhledem k výsledkům analýzy rizik bude společnosti doporučeno v prvotní fázi zavádění bezpečnostních opatření plné akceptování rizik s mírou bezvýznamná, akceptovatelná a nízká. Rizika s mírou nežádoucí a nepřijatelná bude doporučeno ošetřit a jejich ošetření prioritizovat dle výsledků zjištěných v matici rizik. Dle těchto výsledků bude tedy doporučeno prvně ošetřit riziko odcizení klientských dat prostřednictvím emailové služby, jelikož podle dosažených výsledků je toto riziko nejmarkantnější. Po ošetření tohoto rizika bude následovat doporučení na ošetření výpadku internetového připojení vzhledem k funkčnosti emailové služby a také cloudových služeb. Jako třetí bude ošetřeno možné riziko zneužití oprávnění k přístupu ke klientským datům. V rámci rozsahu diplomové práce bude navrhnuto jen opatření pro nejrizikovější část, kterou je již zmíněné odcizení klientských dat prostřednictvím emailové služby.

3.2.2 Návrh vhodného řešení

Do návrhu vhodných řešení budou zahrnuty služby a možná technická řešení tak, aby se od sebe lišily především svým principem fungování. Na trhu lze v dnešní době najít spoustu služeb, poskytujících šifrování emailové komunikace, přičemž se ale od sebe tyto služby liší v zásadě jen systémem šifrování a způsobem zasílání dat, ovšem způsob zacházení s danou službou a hlavní princip fungování je u všech těchto služeb víceméně podobný. Z tohoto důvodu byla vybrána následující tři možná řešení:

- Tresorit
- S/Mime
- Vlastní služba

Jedná se o tři principiálně odlišná řešení, která však svým způsobem fungování dokážou přinést žádaný efekt a to zabezpečení přenosu klientských dokumentů, mezi klientem a společností, které obsahují citlivé informace a u jejichž přenosu je více než vhodné dbát na zabezpečení.

3.2.3 Popis vybraných řešení

V této části práce budou popsána jednotlivá možná řešení, prostřednictvím kterých by bylo možné zavést bezpečnostní opatření na zjištěnou zranitelnost během zasílání klientských dokumentů.

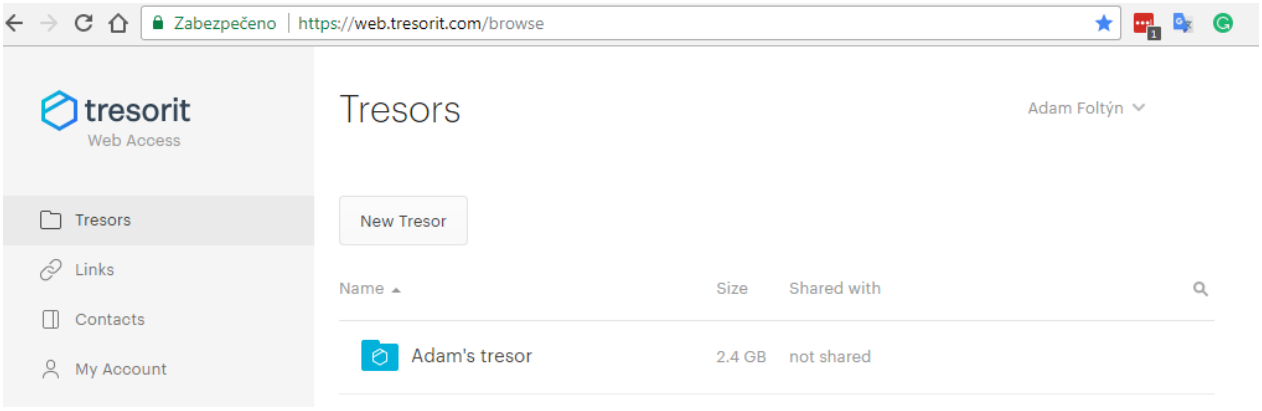
Tresorit

Jako první možnou variantu pro zabezpečení přenosu citlivých dat mezi klientem a společností se nabízí využití řešení od společnosti Tresorit.

Obrázek 11: Tresorit logo (Zdroj: 16)

Společnost Tresorit je švýcarsko-maďarská IT firma, založená roku 2011, jejímž hlavním zaměřením je vývoj stejnojmenného produktu Tresorit, který je šifrovaným cloudovým úložištěm. Tresorit využívá princip end-to-end šifrování, což znamená, že odesílaná data jsou šifrována na úrovni uživatele a do internetu, potažmo cloudu jsou odesílána v již zašifrované podobě. Na rozdíl od klasických nešifrovaných cloudových úložišť tak odpadá riziko možného přístupu a zneužití klientských dat ze strany samotného poskytovatele cloudového řešení, jelikož v případě Tresoritu sice má společnost k datům přístup, nicméně už není schopna klientem uložená data rozšifrovat.

Tresorit funguje ve dvou variantách. První z nich je desktopová (popř. mobilní) aplikace a druhou je prostředí webového prohlížeče. Klient se tak ke svým datům, uloženým na cloudovém úložišti, dokáže dostat i z počítače, na kterém nemá aplikaci Tresorit nainstalovánu. Tresorit je nabízen jak běžným uživatelům, tak i korporátnímu, resp. komerčnímu sektoru. Princip fungování je velice jednoduchý a z uživatelského hlediska přívětivý. Klient se pomocí registrovaného emailu a hesla přihlásí ke svému Tresorit účtu, přičemž je standardně vhodné použít i dvoufaktorovou autentizaci, která probíhá prostřednictvím přepsání číselného kódu, vygenerovaného na některé z mobilních aplikací (např. Google authenticator), která je s daným uživatelským Tresorit účtem propojena. Klientovi se poté zobrazí seznam všech jeho „tresorů" – šifrovaných složek na cloudovém úložišti, které vytvořil buď on sám, nebo mu byly nasdíleny jinými uživateli Tresoritu. V takovýchto tresorech poté může klient vytvářet neomezené množství podsložek a do nich poté nahrávat své dokumenty. Sdílení je možné jak na úrovni tresorů, podsložek tak i jednotlivých souborů. Jak již bylo zmíněno, při nahrávání souborů je aplikováno šifrování na úrovni klienta a to konkrétně metoda symetrického šifrování AES-256. Sdílení šifrovacích klíčů mezi uživateli je poté řešeno pomocí speciálně vyvinutého a patentovaného protokolu přímo od společnosti Tresorit, který kombinuje prvky již zmíněného AES-256 šifrování s klasickým systémem šifrování pomocí veřejných a soukromých klíčů (šifrování pomocí RSA-4096), který stojí na základě infrastruktury správy a distribuce veřejných klíčů PKI (angl. *Public Key Infrastructure*).



Obrázek 12: Prostředí Tresorit (Zdroj: Vlastní)

Jelikož společnost už nyní využívá Tresorit jako své primární uložiště klientských dat, bylo by nahrávání do Tresoritu v rámci úprav firemních procesů uzpůsobeno takovým

způsobem, aby byl poté samotný klient schopen nahrát požadované dokumenty přímo do své předem vytvořené složky na Tresoritu, čímž by se obešel proces zasílání těchto dokumentů přes email. K tomuto úkonu by postačovalo v rámci správy Tresoritu vytvořit několik dodatečných klientských přístupových profilů, na které by byly poté aplikována pouze práva pro nahrávání dokumentů. Takovýto přístup by byl poté zaslán klientovi společně s výzvou a vysvětlením, jak postupovat při nahrávání požadovaných dokumentů.

Celý proces by poté probíhal následovně. Oddělení klientské podpory by po obdržení registračního formuláře, který neobsahuje požadované dokumenty nebo dokumenty, které v rámci schvalovacího procesu nelze akceptovat vytvořilo ve struktuře firemního Tresoritu složku se jménem daného klienta a tuto složku sdílelo s jedním z klientských přístupových profilů. Klient by poté obdržel na email výzvu o nahrání požadovaných dokumentů, popř. dalších doplňujících informací včetně přihlašovacích údajů ke klientskému přístupovému profilu, určeného pro nahrání dokumentů (heslo klientskému přístupovému profilu by bylo zasíláno např. pomocí služby onetimesecret, pomocí které lze zaslat heslo ke službě a po prvním zobrazení již není možné link nadále využívat). Klient by se poté dle přiložených instrukcí přihlásil do Tresoritu (díky nastaveným právům pro daný účet by viděl pouze předem vytvořenou složku se svým jménem) a nahrál požadované dokumenty. Následně by prostřednictvím emailové zprávy informoval oddělení klientské podpory o skutečnosti, že dokumenty nahrál. Oddělení klientské podpory by poté dokumenty zkontrolovalo a v případě, že by dokumenty stále nesplňovaly dané požadavky, bylo by nutné informovat klienta o nutnosti jejich opětovného nahrání. Jakmile by byly dokumenty schváleny, oddělení klientské podpory by změnilo přístupové heslo k vydanému klientskému přístupovému profilu a taktéž by bylo zrušeno sdílení klientské složky do tohoto profilu. Průběh registrace by poté pokračoval standardně.

Mezi kritické činnosti implementace, na které by bylo nutné brát zřetel, patří především poskytnutí práv operátorům oddělení klientské podpory v rámci služby Tresorit tak, aby v případě potřeby mohli založit dodatečný klientský přístupový profil. Dále by bylo nutné vést společnou evidenci klientských přístupových profilů tak, aby bylo možné kdykoliv zjistit, který z profilů se momentálně využívá a je nabízen klientovi. Jako další nezbytnou věc by bylo také nutné vést společnou evidenci dočasných hesel k přístupovým profilům,

aby bylo možné heslo případně opětovně zaslat klientovi, pokud by to situace vyžadovala. Další nezbytné činnosti pro úspěšné provedení implementace jsou poté zaškolení zaměstnanců a tvorba emailové šablony, která bude zasílána klientům a která bude obsahovat vysvětlení nového procesu nahrávání dokumentů.

Náročnost implementace by tedy spočívala především v úpravě současných firemních procesů a zaškolení zaměstnanců, přičemž vhodná doba pro nasazení nového řešení by byla během víkendu, kdy by všechny nové registrační žádosti podané od určitého data (pondělí po víkendu nasazení) byly zpracovávány dle nového procesu. Z časového hlediska je tedy nutné vzít v potaz pouze zaškolení zaměstnanců, kteří jsou však na práci v prostředí Tresoritu zvyklí a jednalo by se tedy jen o vysvětlení nového procesu, které by trvalo maximálně několik jednotek hodin. Dále by bylo nutné vytvořit potřebné evidence aktuálně používaných přístupových profilů a jejich hesel společně se šablonou emailu. Všechny tyto činnosti by neměly překročit dobu trvání 1 MD (z angl. *man-day*).

Jelikož má společnost zakoupenou business licenci Tresoritu a díky vyjednání lepších podmínek platí v současnosti 6 USD za uživatele měsíčně (účtováno ročně) namísto standardních 10 USD. Po konzultaci s oddělením klientské podpory bylo zjištěno, že za dobu existence firmy se počet současně rozpracovaných registračních žádostí, u kterých se nějakým způsobem čeká na dodání dokumentů, pohybuje kolem průměrné hodnoty 20 registrací. Navrhuji tedy vytvoření 40 nových klientských přístupových profilů pro potřeby krytí těchto registrací, přičemž jejich tvorba je plně v rukou společnosti a v případě potřeby zvýšení počtu přístupů je společnost schopna pružně reagovat. Cena tohoto řešení by tak sestávala pouze z vytvoření nových klientských přístupových profilů o celkové ceně 240 USD (měsíčně), což při současném kurzu 20.5 USD/CZK odpovídá přibližně částce 59 000 CZK ročně.

Mezi hlavní výhody tohoto řešení patří nízká časová náročnost implementace za využití stávajících služeb. Mezi nevýhody řadím především složitější postup procesu registrace na straně klienta i zaměstnanců oproti současnému stavu a také využití aplikace třetí strany, která nemusí budit v klientech důvěru.

Celkové hodnocení tohoto řešení poté shrnuje následující tabulka, přičemž hodnocení přívětivosti bylo provedeno na základě subjektivního posouzení autora práce a je vyjádřeno jako počet dosažených bodů z maxima možných.

Tabulka 10: Tresorit shrnutí (Zdroj: Vlastní)

Tresorit	
Typ řešení	cloudové úložiště poskytované třetí stranou
Operátorská přívětivost	3/5
Klientská přívětivost	4/5
Kritické činnosti	- poskytnutí práv operátorům odd. kl. podpory - tvorba evidence pro správu používaných profilů - tvorba evidence pro správu aktuálních hesel - zaškolení zaměstnanců - tvorba emailové šablony s novým postupem
Časová náročnost implementace	1 MD
Cena řešení	59 000 CZK / rok (při původním návrhu vytvoření 40 klientských přístupových profilů)
Výhody	- časová náročnost - využití stávajících služeb
Nevýhody	- složitější proces - využívání aplikace třetí strany

S/MIME

Jako další řešení pro použití v rámci zavedení bezpečnostního opatření při zasílání klientských dokumentů se nabízí využití široce používaného šifrovacího standardu S/MIME, jenž je prověřeným standardem pro šifrování emailové komunikace.

Obrázek 13: S/MIME logo (Zdroj: 17)

Šifrovací standard S/MIME je založen na principu end-to-end šifrování, kdy dochází k zašifrování emailové zprávy na úrovni klienta a email jako takový je poté na poštovní servery zasílán už v šifrované podobě. Hlavní výhoda tohoto typu šifrování emailových zpráv tkví v tom, že k šifrování dochází na úrovni klienta, přičemž lze k šifrování a dešifrování využít rozdílné služby na obou stranách komunikačního kanálu, které poskytují podporu využívání daného standardu. Zpráva je tak šifrována na klientském zařízení a nikoliv až na serveru, přičemž email zaslaný do prostředí internetu tak není závislý na určitém typu poštovního serveru a lze takto zašifrovanou zprávu posílat jako běžný nešifrovaný email.

Počátek historie standardu S/MIME se datuje do roku 1995, kdy byla vyvinuta jeho první verze. Jednalo se tehdy o jedno z několika možných řešení a nešlo tedy zatím o standard. Situace se změnila v roce 1998, kdy byla vydána druhá verze tohoto řešení a v témže roce byla rovněž podána žádost k organizaci IETF (Internet Engineering Task Force) o uznání S/MIME řešení jako internetového standardu. Po jejím schválení se stal standard S/MIME standardním řešením pro šifrování emailové komunikace v rámci internetu. O rok poté v roce 1999 byla vydána třetí verze tohoto již standardu, která je s postupnými úpravami aktuální dodnes.

Jádrem standardu S/MIME je propojení a nabízení dvou bezpečnostních služeb v rámci jednoho řešení. Konkrétně se jedná o:

- Elektronický podpis,
- Šifrování zpráv.

Standard S/MIME obsahuje i další bezpečnostní prvky, nicméně základní funkčnost tvoří dvě výše uvedené služby, které jsou zbylými prvky podporovány. Pro potřeby diplomové práce bude tedy popis funkčnosti daného standardu omezen na vysvětlení dvou zmíněných služeb – elektronického podpisu a šifrování zpráv.

Jak již bylo uvedeno, standard S/MIME funguje na principu end-to-end šifrování za využití PKI (Public Key Infrastructure), kdy je zpráva šifrována na zařízení odesílatele a dešifrována do původní podoby po obdržení na zařízení příjemce. Jako systém šifrování je zde použit osvědčený princip veřejných a soukromých klíčů, kdy je zpráva šifrována pomocí symetrického šifrování a klíč vygenerovaný k tomuto symetrickému šifrování je poté zašifrován pomocí veřejného klíče příjemce, který je veřejně znám a distribuován. Příjemce je poté schopen za pomoci svého privátního klíče, který je soukromý a nesdílený takto zašifrovaný symetrický klíč ke zprávě dešifrovat a za pomocí něho poté dešifrovat již samotnou zprávu.

Šifrování zprávy jako takové poté zaručuje její důvěrnost – po zašifrování víme, že jen její příjemce, který je držitel svého privátního klíče, který náleží k veřejnému klíči, kterým byla zpráva zašifrována, bude schopen danou zprávu dešifrovat. Pouhé šifrování ovšem nezaručuje datovou integritu, tedy jistotu, že šifrovaná zpráva nebyla během doručování v rámci internetového prostředí pozměněna a nepopiratelnost, což je stav, kdy jsme schopni jasně určit odesilatele zprávy, který odeslání zprávy nemůže popřít. Proto se v rámci standardu nepracuje pouze s šifrováním samotným, nýbrž je přidána služba elektronického podpisu, který sám o sobě přidává v rámci řešení prvek nepopiratelnosti a společně s šifrováním i prvek datové integrity.

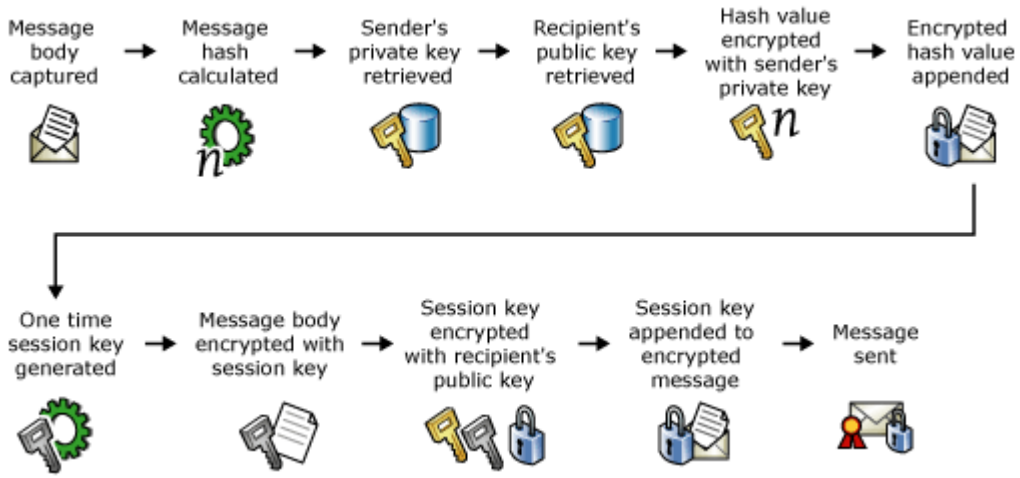
Elektronické podepsání emailu poté probíhá za pomoci vygenerování hashe napsané zprávy, který je následně zašifrován pomocí privátního klíče odesílatele a přiložen k emailu. Příjemce si poté po obdržení emailu extrahuje část zprávy, ze které je spočítán hash a následně pomocí veřejného klíče odesílatele dešifruje zašifrovaný hash. Pokud se pak dešifrovaný hash shoduje s hashem zprávy, který byl vypočítán, je prokázáno, že zpráva byla zaslána konkrétním uživatelem, jehož veřejný klíč byl použit pro dešifrování hashe a také, že zpráva nebyla jakkoliv upravena jelikož zašifrovaný hash vypočítaný z původní zprávy na straně odesilatele se shoduje s hashem příchozí zprávy. Tímto způsobem tak byl do zprávy přidán prvek datové integrity i nepopiratelnosti současně.

Celý proces včetně šifrování samotné zprávy poté funguje následovně. Zpráva je napsána odesílatelem a hash této zprávy je spočítán. Spočítaný hash je poté zašifrován pomocí soukromého klíče odesílatele a přidán ke zprávě jako digitální podpis. Náhodný dočasný klíč pro symetrické šifrování je vygenerován a pomocí něj je zašifrováno tělo zprávy.

Dočasný klíč je poté zašifrován pomocí veřejného klíče příjemce a přiložen ke zprávě. Zpráva je poté odeslána příjemci. Příjemce zprávy po jejím obdržení od sebe nejdříve extrahuje tělo zprávy a zašifrovaný dočasný klíč. Pomocí svého soukromého klíče dešifruje dočasný klíč a za pomoci něj dešifruje také tělo zprávy, od kterého extrahuje přiložený elektronický podpis v podobě šifrovaného hashe. Je spočítán hash obdržené zprávy a pomocí veřejného klíče odesílatele je dešifrován přiložený hash. Na základě porovnání hashů je poté známo, zdali byla zpráva zaslána právoplatným odesílatelem nebo zdali byla během přenosu nějakým způsobem upravena či nikoli a lze ji tak považovat za důvěryhodnou.

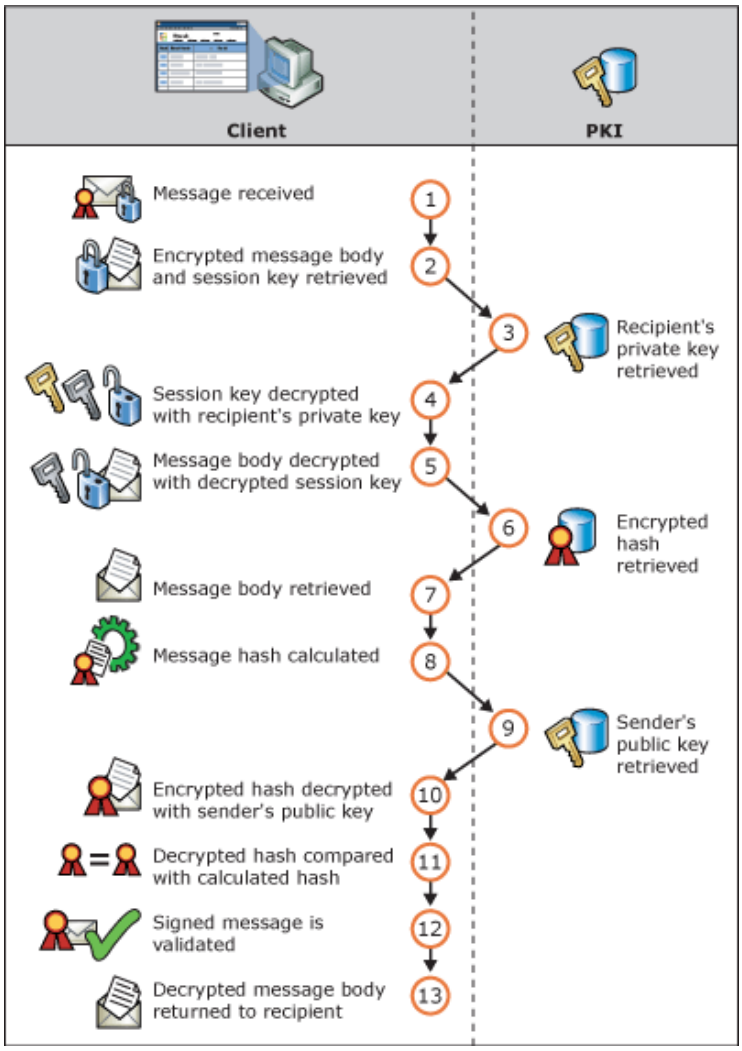
Pro lepší ilustraci obou procesů poté slouží následující dva obrázky.

Proces odeslání šifrované zprávy prostřednictvím standardu S/MIME:



Obrázek 14: S/MIME proces šifrování a odeslání zprávy (Zdroj: 18)

Následný proces dešifrování přijaté zprávy prostřednictvím standardu S/MIME:



Obrázek 15: S/MIME proces přijetí a dešifrování zprávy (Zdroj: 19)

Společnost již v současnosti využívá standard S/MIME pro šifrování vnitropodnikové emailové komunikace. Jako emailový klient je využíván produkt Thunderbird a tudíž by po případném nasazení tohoto řešení nenastaly v rámci procesů na oddělení klientské podpory žádné významné změny. Bylo by pouze nutné při prvním emailovém kontaktu klienta informovat o způsobu šifrované emailové komunikace za využití některé ze služeb, poskytujících podporu pro standard S/MIME, přičemž by byl klient nucen mít naistalovánu tuto službu na svém osobním počítači a také by muselo dojít k vzájemné výměně veřejných klíčů prostřednictvím certifikátů a to pouze za předpokladu, že klient má na své straně již svůj privátní a veřejný klíč vygenerován. Změny na úrovni procesů by poté spočívaly pouze v tom, že by operátor (za předpokladu již vyměněných veřejných klíčů mezi společností a klientem) odesílal veškerou emailovou komunikaci jako šifrovanou a to stejné by bylo prováděno ze strany klienta. Celý registrační proces by tak

probíhal téměř totožně, jako je tomu v současnosti, pouze s výjimkou nutnosti informovat a navést klienta při zřizování a nastavování šifrované komunikace na jeho straně.

Mezi kritické činnosti této implementace by zcela jistě spadalo nalezení vhodného způsobu komunikace s klientem při vysvětlování celého procesu a nutnosti celý proces zřízení šifrované emailové komunikace podstupovat.

Jelikož je standard S/MIME již ve společnost využíván, časová náročnost na implementaci by byla nulová, stejně tak jako náklady na jeho provozování, jelikož využívaný klient Thunderbird je dostupný jako freeware a jeho využívání není zpoplatněno ani v rámci komerčního sektoru. Klíče jsou poté generovány mateřskou společností, jenž figuruje jako certifikační autorita a tudíž je i vydávání certifikátů pro potřeby zaměstnaneckých účtů společnosti zdarma.

Mezi výhody tohoto řešení patří jednoznačně nulové náklady a možnost téměř okamžitého zavedení po nalezení vhodného způsobu, jak klientovi potřebu tohoto druhu komunikace vysvětlit i s jasným návodem, jak postupovat. Mezi nevýhody se řadí velká technická zátěž, která by byla kladena na klienta při zřizování a nastavování komunikace a také nutnost využití aplikace třetí strany (některého emailového klienta podporujícího standard S/MIME) na klientově straně.

Celkové hodnocení tohoto řešení poté opět shrnuje tabulka, přičemž hodnocení přívětivosti bylo provedeno na základě subjektivního posouzení autora práce a je vyjádřeno jako počet dosažených bodů z maxima možných.

Tabulka 11: S/MIME shrnutí (Zdroj: Vlastní)

S/MIME	
Typ řešení	šifrovací standard pro emailovou komunikaci
Operátorská přívětivost	4/5
Klientská přívětivost	1/5
Kritické činnosti	- vysvětlení nutnosti tohoto opatření klientovi - tvorba kvalitního manuálu pro klienta
Časová náročnost implementace	0 MD - řádově jednotky hodin
Cena řešení	0 CZK / rok
Výhody	- časová, téměř nulová náročnost implementace - nulové provozní náklady díky použití freewaru
Nevýhody	- složitý postup na straně klienta - využívání aplikace třetí strany

Klientská zóna

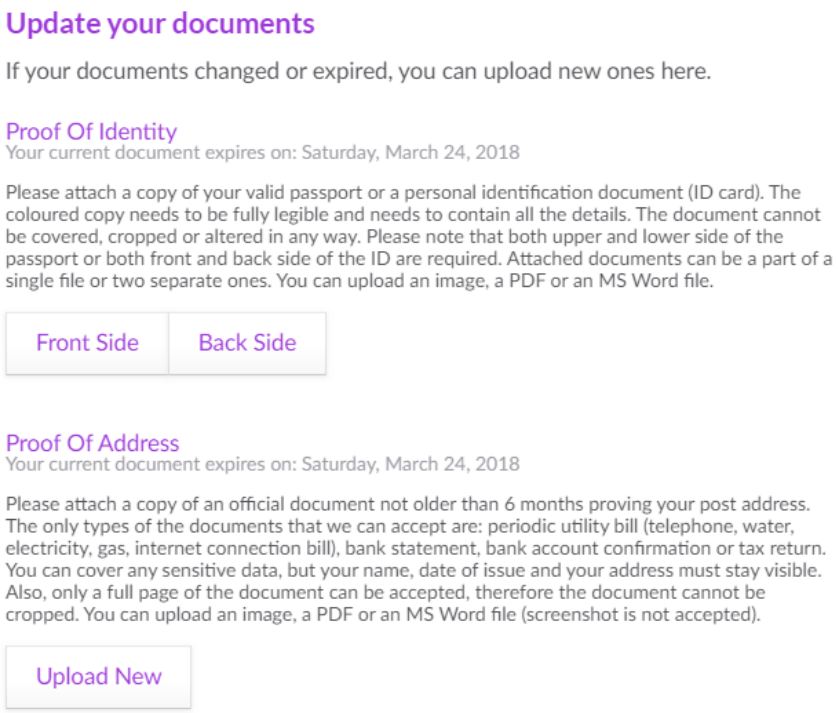
Třetí potenciální variantou, jak zabezpečit přenos citlivých dokumentů mezi klientem a společností během procesu registrace je naprogramování, resp. úprava stávajícího vlastního webového řešení pro účely registrace nového klienta.

Obrázek 16: Klientská zóna logo (Zdroj: Vlastní)

Vlastní webové rozhraní nebo služba, prostřednictvím které lze nahrát dokumenty ke zpracování přímo do systému společnosti, která je od klienta požaduje, se stává v dnešní době již standardem a lze se s tímto způsobem nahrávání dokumentů setkat jak u velkých finančních společností, kterými jsou banky nebo pojišťovny, tak i u menších společností

poskytujících služby jakéhokoliv druhu. Tento systém funguje na jednoduchém principu, kdy je klientovi vytvořen účet v rámci určitého back office rozhraní, do kterého se klient poté svými přihlašovacími údaji přihlásí a může zde vykonávat nejrůznější operace včetně samotného nahrávání dokumentů a jejich správy.

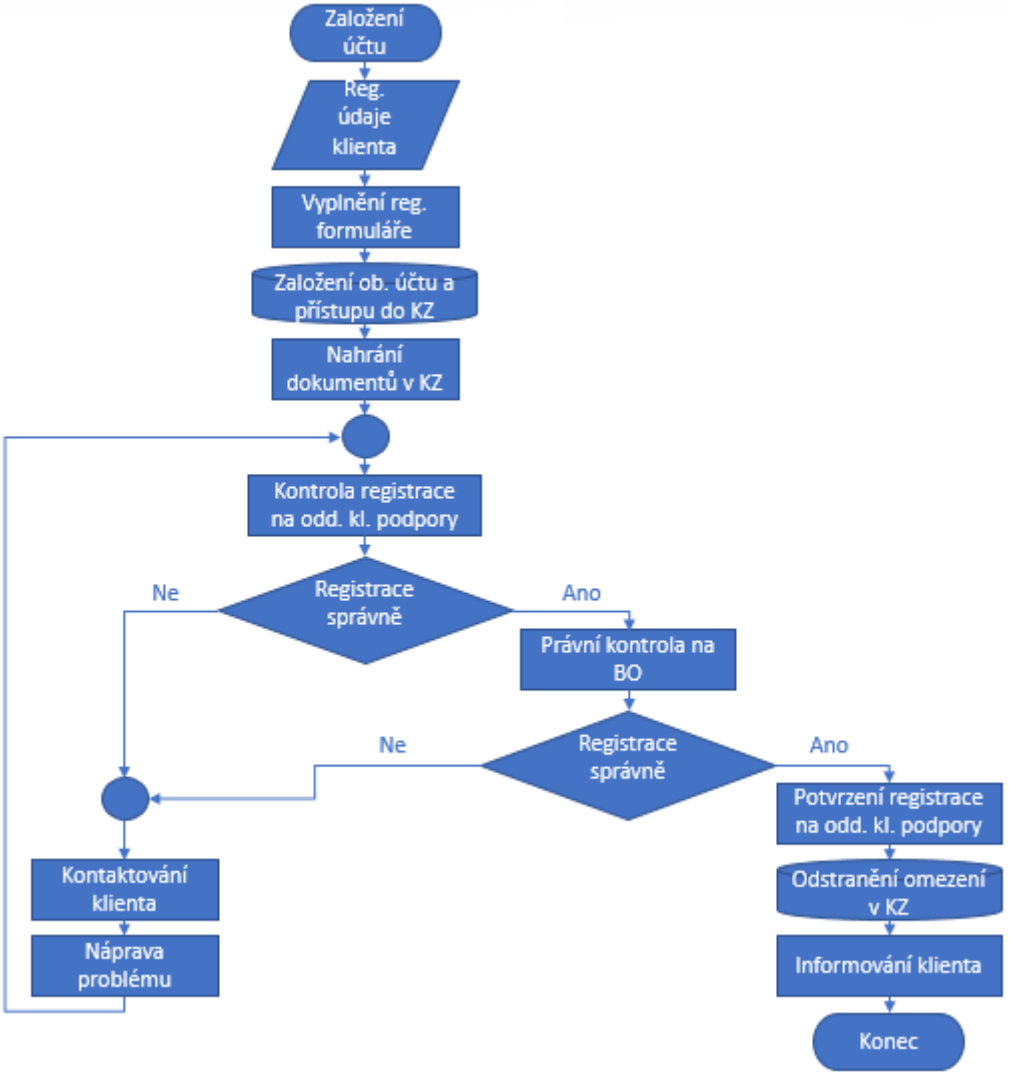
Společnost Obchodní s.r.o. již v současné době využívá klientskou zónu, do které mají přístup registrovaní klienti a která slouží k nejrůznějším klientským činnostem tak, aby byl klient schopen si v rámci svého uživatelského profilu nebo svých jednotlivých obchodních účtů provést určitá nastavení, která by byla v opačném případě nutná provádět za asistence oddělení klientské podpory. Jedná se například o možnost založení dalšího obchodního účtu, nastavení parametrů současných obchodních účtů, provádění finančních operací jako jsou převody mezi obchodními účty, zadávání požadavků na výběr finančních prostředků a další možnosti. Hlavní funkcionalitou je ovšem možnost nahrání a správa klientských dokumentů, které jsou poté pomocí šifrovaného přenosu nahrány rovnou do firemní databáze a odtud poté přesunuty pomocí API rozhraní na šifrované cloudové úložiště Tresorit. Klient poté vidí ve své klientské zóně v sekci Osobní dokumenty data exspirace jednotlivých nahraných dokumentů a v případě, že je vyzván k jejich opětovnému doložení, využije nahrávací funkce klientské zóny.



Obrázek 17: Klientská zóna - prostředí (Zdroj: Vlastní)

V rámci návrhu využití stávající klientské zóny jako bezpečnostního opatření je zapotřebí vzít do úvahy fakt, že ve stávající podobě slouží klientská zóna pouze již registrovaným klientům a klienti s nedokončenou registrací do ní nemají přístup, neboť ten je klientovi přidělen až poté, co je dokončena jeho registrace. Zavedení možnosti nahrávat klientské dokumenty prostřednictvím klientské zóny je tak při stávajícím řešení otázkou procesního řízení, kdy by bylo zapotřebí upravit chod jednotlivých procesů při zachování současné podoby a funkčnosti klientské zóny pouze s jejími drobnými úpravami.

Proces registrace by byl poté následovný. Z registračního online formuláře, který klient vyplňuje, by byla odstraněna část, ve které je po klientovi požadováno nahrání citlivých dokumentů a klient by tak vyplnil pouze požadované písemné údaje o své osobě, jeho finanční situaci a údaje o bydlišti. Na místo odstraněné části by bylo umístěno oznámení, že dokončení celého registračního procesu bude provedeno prostřednictvím klientské zóny. Na základě informací, vyplněných v registračním formuláři by byl poté klientovi založen obchodní účet včetně přístupu do klientské zóny, který by byl zároveň zaslán a na uvedenou emailovou adresu klienta včetně požadavku a postupu ohledně nahrání požadovaných dokumentů. Klient by se poté mohl přihlásit do klientské zóny, kde by viděl, že má svůj obchodní účet již založený. V případě požadavku na vložení finančních prostředků by byl klient klientskou zónou informován, že jeho registrace není kompletní a je zapotřebí dodat požadované dokumenty prostřednictvím sekce Osobní dokumenty. Jakmile by klient nahrál požadované dokumenty, do ticketového systému oddělení klientské podpory by byl automaticky vytvořen požadavek na kontrolu registrace a proces verifikace by probíhal stejným způsobem jako za současného stavu, tj. byla by provedena kontrola celé registrace pracovníkem oddělení klientské podpory, v případě schválení by byla registrace postoupena na oddělení back office, kde by proběhla závěrečná kontrola registrace. Po schválení registrace by poté bylo klientovi z jeho klientské zóny odstraněno omezení na provedení vkladu a tím by mu bylo umožněno využívat klientskou zónu v plném rozsahu jako je tomu nyní u již registrovaných klientů.



Obrázek 18: Upravený proces registrace (Zdroj: Vlastní)

Mezi kritické činnosti této implementace patří především zajištění možnosti vkládat finanční prostředky skrze klientskou zónu teprve až po nahrání požadovaných dokumentů a schválení celé registrace. Dále je také nezbytné upravit stávající automatický registrační systém takovým způsobem, aby docházelo k zakládání obchodních účtů a tím i přístupů do klientské zóny již po obdržení vyplněného registračního formuláře.

Časová náročnost úpravy stávajícího registračního systému takovým způsobem, aby odpovídal požadovanému stavu je vedoucím pracovníkem developerského týmu odhadována na 8 MD. V rámci tohoto časového úseku by také došlo k zaškolení zaměstnanců oddělení klientské podpory, kdy by byli operátoři obeznámeni s novým procesem a funkčností klientské zóny. Jelikož si společnost obstarává vývoj softwarových řešení pomocí outsourcingu z jiné společnosti v rámci téhož holdingu, bylo

by zapotřebí vznést požadavek na úpravu klientské zóny a registračního systému právě do této společnosti. Společnost vyvíjející software pro Obchodní s.r.o. obstarává vývojářskou činnost i pro další společnosti v rámci holdingu a nelze tak počítat s okamžitým provedením požadovaných změn. Délka čekání na zpracování tohoto projektu je pak odhadována na základě předchozích zkušeností s podobnými úkony vedením společnosti na 4 – 5 měsíců, což je průměrná doba, kdy se vývojářská společnost dostane do stavu, kdy bude mít volné kapacity pro účely provedení požadovaných změn v rámci navrhovaného řešení.

Cena implementace by se poté skládala pouze z jedné položky. Tou je platba za úpravu registračního systému senior web developerovi, jehož hodinová sazba se pohybuje okolo 250 CZK, což při 8 MD jednotkách činí výslednou částku 16 000 CZK.

Výhodou této implementace je její relativní jednoduchost na provedení, kdy jsou veškeré systémové změny realizovány samotnými developery klientské zóny, což s sebou přináší i možnosti případných úprav, kdyby se v rámci nového procesu vyskytly chyby. Další výhodou je poté samotné využívání vlastní služby, kdy není společnost vázána na službu třetí strany a tím se zvyšuje kredibilita samotné společnosti. Navrhované řešení je navíc uživatelsky velice přívětivé jak pro stranu klienta, tak i pro stranu zaměstnanců, kde nedojde k žádným razantním procesním změnám. Nevýhodou tohoto řešení je delší časová náročnost, způsobená především dlouhou čekací dobou na zpracování požadavku ze strany vývojářské společnosti.

Celkové hodnocení této implementace je shrnuto v následující tabulce, přičemž hodnocení přívětivosti bylo provedeno na základě subjektivního posouzení autora práce a je vyjádřeno jako počet dosažených bodů z maxima možných.

Tabulka 12: Klientská zóna shrnutí (Zdroj: Vlastní)

Klientská zóna	
Typ řešení	vlastní webová služba
Operátorská přívětivost	5/5
Klientská přívětivost	5/5
Kritické činnosti	- ošetření správné funkčnosti klientské zóny - úprava registračního systému
Časová náročnost implementace	4 - 5 měsíců čekací lhůta + 8 MD implementace
Cena řešení	16 000 CZK
Výhody	- jednoduchost implementace - vlastní řešení - uživatelská přívětivost
Nevýhody	- delší časová náročnost implementace

3.2.4 Srovnání vybraných řešení

Na základě popisu každého z navrhovaných řešení byla sestavena následující tabulka, shrnující sledované parametry u jednotlivých řešení. Zvýraznění pozitivních parametrů, které autor dle svého subjektivního uvážení zvolil jako klíčové a které výraznou měrou ovlivňují finální rozhodování, je provedeno zeleným podbarvením a naopak podbarvení červenou barvou značí klíčový negativní parametr.

Tabulka 13: Srovnání vybraných řešení (Zdroj: Vlastní)

Parametry	Tresorit	S/MIME	Klientská zóna
Typ řešení	cloudové úložiště poskytované třetí stranou	šifrovací standard pro emailovou komunikaci	vlastní webová služba
Operátorská přívětivost	3/5	4/5	5/5
Klientská přívětivost	4/5	1/5	5/5
Kritické činnosti	- poskytnutí práv operátorům odd. kl. podpory - tvorba evidence pro správu používaných profilů - tvorba evidence pro správu aktuálních hesel - zaškolení zaměstnanců - tvorba emailové šablony s novým postupem	- vysvětlení nutnosti tohoto opatření klientovi - tvorba kvalitního manuálu pro klienta	- ošetření správné funkčnosti klientské zóny - úprava registračního systému
Časová náročnost implementace	1 MD	0 MD - řádově jednotky hodin	4 - 5 měsíců čekací lhůta + 8 MD implementace
Cena řešení	59 000 CZK / rok (při původním návrhu vytvoření 40 klientských přístupových profilů)	0 CZK / rok	16 000 CZK
Výhody	- časová náročnost - využití stávajících služeb	- časová, téměř nulová náročnost implementace - nulové provozní náklady díky použití freewaru	- jednoduchost implementace - vlastní řešení - uživatelská přívětivost
Nevýhody	- složitější proces - využívání aplikace třetí strany	- složitý postup na straně klienta - využívání aplikace třetí strany	- delší časová náročnost implementace

3.2.5 Akvizice řešení

Na základě popisu a srovnání parametrů jednotlivých řešení byly vyvozeny následující závěry, pro každé z navrhovaných řešení.

Služba Tresorit by po zavedení plně splňovala nároky na zabezpečenou komunikaci v rámci předávání citlivých dokumentů mezi klientem a společností. Proces nahrávání dokumentů by byl pro klienta o něco méně pohodlný, než je tomu doposud prostřednictvím emailové komunikace. Oproti tomu by se na druhou stranu značně zkomplikoval proces registrace na straně oddělení klientské podpory, které by muselo vykonávat a ošetřit několik kritických činností, jakými jsou správa přístupových klientských profilů a k nim příslušejícím heslům. Velké pozitivum je spatřováno v možnosti téměř okamžitého nasazení řešení při využívání stávající služby, kdy je tato vlastnost negativně kompenzována cenovou náročností implementace a provozu, který je ze všech vybraných řešení finančně nejvíce nákladný. Dalším faktorem je využití samotné služby Tresorit, jenž je aplikací třetí strany a ta se může klientům jevit jako méně důvěryhodná.

Zabezpečení komunikace prostřednictvím využití šifrovacího standardu S/MIME se jeví jako vhodné a zcela automatické řešení, jelikož proces registrace by zůstal nezměněn a na straně oddělení klientské podpory by došlo pouze k přechodu ve využívání jiného emailového klienta Thunderbird, se kterým mají operátoři již bohaté zkušenosti. Dalšími pozitivními faktory pro výběr tohoto řešení se jeví také časová náročnost implementace, která se pohybuje v řádech jednotek hodin včetně ceny samotného řešení, která je nulová díky využívání freewarového emailového klienta. Toto řešení by ovšem mělo velice negativní dopad na stranu potenciálního klienta, jelikož by byl klient nucen k instalaci aplikace třetí strany – emailového klienta a jeho nastavení.

Třetím řešením je poté využití stávající klientské zóny za předpokladu jejích drobných úprav společně s minimální úpravou registračního procesu jak na úrovní jeho řízení, tak i na úrovni systému. Kritické činnosti této implementace tak spočívají především v úpravách registračního systému a klientské zóny, které by byly ovšem prováděny jejími samotnými vývojáři. Výhodou této implementace je především velká uživatelská přívětivost na straně klienta za využití vlastní služby. Proces registrace by zůstal pouze s malými změnami totožný i pro oddělení klientské podpory. Nevýhodou tohoto řešení je

poté jeho časová náročnost z důvodu čekání na uvolnění zdrojů v rámci vývojářského týmu.

Po konzultaci s vedením společnosti bylo dospěno k závěru, že řešení pomocí šifrovacího standardu S/MIME není pro potřeby společnosti vyhovující. Navzdory všem svým pozitivům klade velké technické požadavky na stranu klienta, a jelikož společnost Obchodní s.r.o. je velice pro-klientsky orientovaná, nechce dopustit případnou ztrátu klientů z důvodu nevhodně zvoleného technického řešení na své straně a tím pádem i špatně nastaveného procesu komunikace.

Pro firmu tak bylo nakonec navrženo využití jak řešení prostřednictvím cloudového úložiště Tresorit, tak i řešení využívající klientskou zónu s upravenou funkcionalitou. Jelikož dne 25.5.2018 vstupuje v platnost evropské nařízení na ochranu osobních údajů GDPR a společnost Obchodní s.r.o. nebude do té doby schopna upravit současnou podobu klientské zóny takovým způsobem, aby odpovídal požadovanému stavu v rámci navrhovaného řešení, bylo rozhodnuto, že po dobu, během které se bude čekat na uvolnění zdrojů ve vývojářské společnosti, jenž bude klientskou zónu upravovat a taky během doby trvání samotné úpravy, bude nasazeno provizorní řešení za využití služby Tresorit.

Ve výsledku se tak bude jednat o dočasné nasazení služby Tresorit jako prostředku pro předávání citlivých dokumentů, mezitím co se bude pracovat na úpravách klientské zóny, která po prodělaných úpravách Tresoritové řešení zcela nahradí. Dojde tak ke splnění požadavku na zabezpečení předávání citlivých dokumentů ze strany klienta do společnosti za využití nejprve služby třetí strany a později za plného využití služby vlastní.

Možné schéma zavedení vybraných řešení do provozu shrnuje následující diagram.

Tabulka 14: Diagram činností (Zdroj: Vlastní)

1.3.2018		25.5.2018		1.8.2018	
Tresorit - zavádění řešení		Tresorit - využívání řešení		Tresorit - ukončení využívání	
Kl. zóna - modifikace		Kl. zóna - modifikace a zavádění		Kl. zóna - využívání řešení	
Hlavní činnosti		Hlavní činnosti		Hlavní činnosti	
Tresorit	**Kl. zóna**	**Tresorit**	**Kl. zóna**	**Tresorit**	**Kl. zóna**
- tvorba kl. profilů - tvorba evidenci - školení zam. - tvorba email. šab.	- konzultace s dev. odd. - zadání požadavku na vývoj	- správa evidenci - řízení kl. přístupů	- modifikace KZ - testování KZ - úprava informačních materiálů	- zrušení kl. přístupů - záloha evidenci	- monitorování funkčnosti

3.3 Zhodnocení zaváděných opatření

Jelikož je výstupem návrhu bezpečnostních opatření zavedení dvou typů řešení, jejichž funkcionalita je rozdílná, ale z důvodu splnění požadavků na zabezpečení komunikace je tento návrh dvojího řešení nezbytný, skládá se celková ekonomická nákladovost zavedení ze dvou položek.

První z nich je nákladová položka týkající se zavedení dočasného překlenovacího řešení v podobě využití služby Tresorit. Jelikož se ale jedná jen o dočasné řešení, finanční nákladovost na implementaci nebude kalkulována v plném rozsahu, jako by tomu bylo v případě využívání tohoto řešení jako jediného možného. Finanční nákladovost tohoto řešení bude vycházet z předpokladu využití řešení v rozmezí 4 měsíců na celkovou sumu 19 680 CZK. Suma placená každý měsíc za provoz tohoto řešení činí 240 USD, což při současném kurzu 20.5 USD/CZK odpovídá přibližně částce 4 920 CZK měsíčně.

Druhou nákladovou položkou tvoří náklady spojené s modifikací klientské zóny ze strany vývojářské společnosti, jenž byly vyčísleny na 16 000 CZK.

Výsledné finanční náklady na implementaci navrhované kombinace řešení tak činí 35 680 CZK.

Tabulka 15: Finanční náklady (Zdroj: Vlastní)

Finanční náklady			
Typ řešení	**Nákladová položka**	**Počet**	**Cena**
Tresorit	klientské přist. účty	40 účtů na 4 měsíce	19 680 CZK
Klientská zóna	modifikace kl. zóny	vývojář - 8 MD	16 000 CZK
Suma			**35 680 CZK**

Časová náročnost zavedení bezpečnostních opatření poté koresponduje s kalkulacemi pro jednotlivá řešení, kdy lze za celkovou dobu trvání projektu určit modifikaci klientské zóny, jelikož implementace řešení prostřednictvím služby Tresorit bude probíhat simultánně. Tato doba se poté může pohybovat v rozmezí 4 až 5 měsíců čekací lhůty a osm pracovních dní na samotnou implementaci.

Tabulka 16: Časová náročnost (Zdroj: Vlastní)

Časová náročnost			
Typ řešení	**Počet MD**	**Čekací lhůta na implementaci**	**Celkem**
Tresorit	1	-	1 MD
Klientská zóna	8	4-5 měsíců	8 MD + čekací lhůta

PŘÍNOSY PRÁCE

Hlavní přínos práce pro její reálné využití spatřuji převážně v tom, že na základě analýzy rizik byla odhalena potenciální informační rizika, kterými by se měla společnost Obchodní s.r.o. zabývat. Už jen samotný fakt, že došlo k odhalení na první pohled ne zcela viditelných zranitelností, na které bylo vedení společnosti upozorněno, jistě přispívá k tomu, že společnost začne svojí informační bezpečnost přezkoumávat, zabývat se jí do hloubky a chápat její celkovou komplexnost a provázanost na úrovni celé společnosti i na sebe navazujících procesů.

Na nejkritičtější odhalenou zranitelnost byly v rámci této práce navrhnuta bezpečnostní opatření, jejich srovnání a následný návrh pro akvizici takovým způsobem, aby se společnost Obchodní s.r.o. mohla při zavádění bezpečnostního opatření na tuto zranitelnost opírat právě o poznatky získané v rámci této práce. Finanční kalkulace společně s časovými odhady implementací jednotlivých bezpečnostních opatření vycházejí z odborných zkušeností a stávajících ceníků, což společnosti může napomoci v případném rozhodování mezi implementací některého z řešení, které v rámci práce nebylo uvedeno a některým z uvedených řešení, pokud by se společnost rozhodovala pro jiný typ bezpečnostního opatření.

Po ošetření všech zjištěných zranitelností může společnost začít uvažovat o zavedení ISMS jako celku a o jeho případné certifikaci dle norem řady ISO 27000, které by ve výsledku vedlo k zefektivnění řízení informační bezpečnosti jako takové. Zavedení a certifikace ISMS by bylo jistě pozitivně vnímáno i samotnými klienty společnosti, což by společnosti Obchodní s.r.o. určitě přidalo na už tak již vysoké důvěryhodnosti.

ZÁVĚR

V rámci své diplomové práce jsem se zabýval návrhem akvizice služby pro zabezpečení emailové komunikace mezi zkoumanou společností a jejími klienty dle ISMS.

V části práce teoretická východiska byly shrnuty a vysvětleny pojmy spojené především s tématy, týkajících se ISMS, emailové komunikace, řízením informační bezpečnosti dle adekvátních norem a analýzou rizik, jenž tvoří základ pro zavedení ISMS do podniku. Byla zde tak vysvětlena teorie nutná pro pochopení dalších dílčích částí práce.

Část práce analýza současného stavu poté představuje společnost včetně předmětu jejího podnikání, organizační struktury a primárních procesů, které tvoří hlavní náplň zaměstnanců společnosti. Je zde popsán stav informační bezpečnosti ve sledované společnosti. Jsou zde sepsána aktiva a využívané nástroje, relevantní vzhledem k informační bezpečnosti. Analýza současného stavu obsahuje také popis řízení přístupu, aspekty fyzického zabezpečení včetně nastavených politik.

Ve třetí návrhové části práce byla zpracována analýza rizik na základě informací zjištěných v analýze současného stavu, ze které vyvstanul požadavek na zabezpečení emailové komunikace mezi společností a jejími klienty. Pro zabezpečení vzniklého rizika jsou zde vybrány tři služby a po jejich následovném porovnání vybrány dvě, vhodné pro doporučení k akvizici.

Praktickým výstupem práce je poté doporučení na akvizici dvou vybraných služeb, pomocích kterých může společnost vhodně zabezpečit emailový komunikační proces mezi společností a klienty společně s odůvodněním jejich výběru a ekonomickým zhodnocením.

Vzhledem k výše uvedenému lze konstatovat, že v rámci práce došlo k naplnění všech předem stanovených cílů.

SEZNAM POUŽITÉ LITERATURY

1. ČSN ISO/IEC 27000 (36 9790). *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.
2. ČSN ISO/IEC 27001 (36 9797). *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.
3. ČSN ISO/IEC 27003 (36 9790). *Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018.
4. DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
5. ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.
6. POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 9788073802769.
7. *Microsoft Azure* [online]. Seattle: Microsoft, © 2018 [cit. 2018-05-03]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-cloud-computing/
8. *Co je GDPR?* [online]. Praha: Mgr. Eva Škorničková [cit. 2018-05-03]. Dostupné z: https://www.gdpr.cz/gdpr/
9. *Microsoft TechNet* [online]. Microsoft, © 2018 [cit. 2018-05-03]. Dostupné z: https://technet.microsoft.com/library/aa995740(v=exchg.65).aspx
10. *How Email Works* [online]. Oslo: Runbox Solutions AS [cit. 2018-05-03]. Dostupné z: https://runbox.com/email-school/how-email-works/
11. *FLOSS Manuals* [online]. Toronto: FLOSS, 2010 [cit. 2018-05-03]. Dostupné z: http://write.flossmanuals.net/thunderbird/how-email-works/
12. *Na co se obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR) vztahuje?* [online]. Evropská unie [cit. 2018-05-03]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_cs

13. *Guidelines for SMEs on the security of personal data processing* [online]. European Union Agency for Network and Information Security, ©2005-2018 [cit. 2018-05-03]. Dostupné z: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing
14. *GDPR Key Changes* [online]. Trunomi [cit. 2018-05-03]. Dostupné z: https://www.eugdpr.org/the-regulation.html
15. ČSN ISO/IEC 27005 (36 9790). *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.
16. *Tresorit* [online]. Tresorit, © 2017 [cit. 2018-05-03]. Dostupné z: https://tresorit.com/blog/new-tresorit-visual-identity/
17. *GitHubGist* [online]. GitHub, © 2018 [cit. 2018-05-03]. Dostupné z: https://gist.github.com/rmoriz/5945400
18. *Microsoft TechNet* [online]. Microsoft, ©2018 [cit. 2018-05-03]. Dostupné z: https://technet.microsoft.com/cs-cz/library/aa998077(v=exchg.65).aspx
19. ČSN ISO/IEC 27002 (36 9798). *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK